

MCE 2-22.1

CONTRAINTTELIGENCIA

JUNIO 2019



EJÉRCITO NACIONAL
DE COLOMBIA

MANUAL DE CAMPAÑA DEL EJÉRCITO
MCE 2-22.1 CONTRAINTELIGENCIA
RESTRINGIDO
Junio 2019

IMPRESO POR
Publicaciones Ejército

Restricciones de distribución: se autoriza su difusión únicamente a las unidades incluidas en la tabla de autorización del CEDOE.

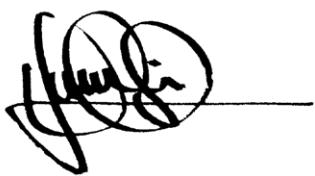
R E S T R I N G I D O
PARA USO EXCLUSIVO DEL CEDOE

MCE 2-22.1
Septiembre de 2019

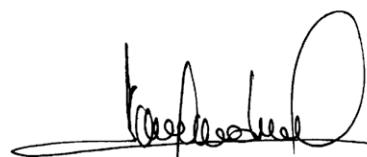


General NICACIO DE JESÚS MARTÍNEZ ESPINEL
Comandante del Ejército Nacional

Autentica:



Coronel PEDRO JAVIER ROJAS GUEVARA
Director Centro de Doctrina del Ejército



Brigadier General ROBINSON A. RAMÍREZ CEDEÑO
Comandante Comando de Educación y Doctrina

Distribución:

El Comandante del Ejército autoriza la distribución del **MANUAL DE CAMPAÑA DEL EJÉRCITO (MCE) 2-22.1, CONTRAINTELIGENCIA**, de acuerdo con lo establecido en respectivo programa directivo, estipulado en el *Reglamento de doctrina y publicaciones militares del Ejército Nacional*, EJC 1-01, de mayo de 2017, capítulo II, sección B, numeral 3, literal j, subnumeral 1), subliteral d). El manual cumplió con el proceso establecido para el desarrollo de publicaciones militares, por lo que se aprueba y autoriza su difusión, acorde con los niveles de clasificación y reserva.

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

FUERZAS MILITARES DE COLOMBIA



EJÉRCITO NACIONAL

**RESOLUCIÓN NÚMERO 001182 DE 2019
(26 DE JUNIO DE 2019)**

Por la cual se aprueba la generación del
**"MANUAL DE CAMPAÑA DEL EJÉRCITO
MCE 2-22.1 CONTRAINTELIGENCIA"**

EL DIRECTOR DEL CENTRO DE DOCTRINA DEL EJÉRCITO

En uso de las atribuciones legales que le confiere en el capítulo III, sección B, numeral 19, literal c) del *Reglamento de doctrina y publicaciones militares del Ejército Nacional EJC 1-01 de 2017* (público), y

CONSIDERANDO:

Que la Dirección de Producción Doctrina, Organización y Equipamiento DIPOE elaboró el proceso de generación del **"MANUAL DE CAMPAÑA DEL EJÉRCITO MCE 2-22.1 CONTRAINTELIGENCIA"**, acorde con lo dispuesto en el *Reglamento de doctrina y publicaciones militares del Ejército Nacional EJC 1-01 de 2017*.

Que el proponente aprobó el citado texto mediante Acta No. 100739 de fecha 09 de mayo de 2019 y plantea que este sea adoptado como **"MANUAL DE CAMPAÑA DEL EJÉRCITO MCE 2-22.1 CONTRAINTELIGENCIA"**.

RESUELVE:

ARTÍCULO 1º Aprobar la generación del **"MANUAL DE CAMPAÑA DEL EJÉRCITO MCE 2-22.1 CONTRAINTELIGENCIA"**, de conformidad con lo establecido en el capítulo II, sección B, numeral 3, literal j, anexo B, literal 2 del *Reglamento de doctrina y publicaciones militares del Ejército Nacional EJC 1-01 de 2017*, el cual se identificará así:

**MANUAL DE CAMPAÑA DEL EJÉRCITO
CONTRAINTELIGENCIA
MCE 2-22.1
RESTRINGIDO
JUNIO 2019**

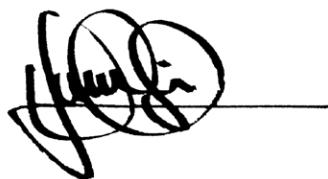
ARTÍCULO 2º La retroalimentación relevante sobre el contenido del manual y las recomendaciones a que dé lugar la aplicación del mismo, deben ser presentadas al Comando de Educación y Doctrina del Ejército Nacional, a fin de estudiarlas y tenerlas en cuenta para su perfeccionamiento conforme lo establece el *Reglamento de doctrina y publicaciones militares del Ejército Nacional EJC 1-01 de 2017* capítulo II, sección B, numeral 4, literal b.

ARTÍCULO 3º Disponer la publicación e implementación del manual aprobado en la presente resolución de acuerdo a lo normado en el capítulo II, sección B, numeral 4, del *Reglamento de doctrina y publicaciones militares del Ejército Nacional EJC 1-01 de 2017*.

ARTÍCULO 4º La presente resolución rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 26 días del mes de junio de 2019.



Coronel PEDRO JAVIER ROJAS GUEVARA
Director del Centro de Doctrina del Ejército

MCE 2-22.1, G

FUERZAS MILITARES DE COLOMBIA

EJÉRCITO NACIONAL



COMANDO DE EDUCACIÓN Y DOCTRINA

Generación

Manual de campaña del Ejército
n.º 2-22.1
Restringido
Junio de 2019

CONTRAINTELIGENCIA

1. La presente publicación es generada como nuevo desarrollo por lo cual aún no se registran cambios.

PÁGINAS MODIFICADAS

PÁGINAS NUEVAS

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

CONTENIDO

INTRODUCCIÓN	xv
CAPÍTULO 1 LA CONTRAINTELIGENCIA	1-1
1.1. FUNDAMENTOS DE LA CONTRAINTELIGENCIA	1-5
1.1.1. Actividades de la contrainteligencia	1-5
1.1.2. Agentes de inteligencia y contrainteligencia	1-8
1.2. COMPETENCIAS DISTINTIVAS DE LA CONTRAINTELIGENCIA	1-10
1.2.1. Seguridad militar	1-11
1.2.2. Operaciones de contrainteligencia	1-11
1.2.3. Cibercontrainteligencia	1-12
1.3. LA CONTRAINTELIGENCIA EN APOYO A LOS NIVELES DE LA GUERRA	1-12
1.3.1. Nivel estratégico	1-13
1.3.2. Nivel operacional	1-24
1.3.3. Nivel táctico	1-26
1.4. LA CONTRAINTELIGENCIA EN LAS OPERACIONES TERRESTRES UNIFICADAS	1-28
1.4.1. La contrainteligencia en la acción unificada	1-29
1.4.2. La contrainteligencia en las tareas de la acción decisiva	1-30
1.4.3. La contrainteligencia en las funciones de conducción de la guerra	1-33
CAPÍTULO 2 ACCIONES DE LA INTELIGENCIA DE LA AMENAZA Y ACCIONES DE RESPUESTA DE LA CONTRAINTELIGENCIA	2-1
2.1. OBJETIVOS DE LA CONTRAINTELIGENCIA	2-2
2.1.1. Espionaje	2-4
2.1.2. Sabotaje	2-6
2.1.3. Subversión	2-7
2.1.4. Terrorismo	2-9
2.1.5. Insurgencia	2-12
2.1.6. Corrupción	2-14

2.2.	RECOLECCIÓN DE INFORMACIÓN DE LA AMENAZA	2-16
2.2.1.	Infiltración	2-17
2.2.2.	Penetración	2-19
2.2.3.	Suplantación	2-20
CAPÍTULO 3 OPERACIONES DE CONTRAINTELIGENCIA		3-1
3.1.	GENERALIDADES	3-2
3.2.	COMPONENTES DE LAS OPERACIONES	3-3
3.3.	OPERACIONES DE CIBERCONTRAINTELIGENCIA	3-6
3.4.	PROCEDIMIENTOS DE CONTRAINTELIGENCIA	3-7
3.4.1.	Procedimiento para el despliegue operacional de contrainteligencia	3-7
3.4.2.	Procedimiento para la integración de actividades en un área específica	3-12
3.4.3.	Procedimiento operacional de contrainteligencia	3-15
3.4.4.	Procedimiento para asignación de analista de contrainteligencia	3-35
3.4.5.	Procedimiento de contraespionaje del equipo rojo	3-40
3.4.6.	Procedimiento de gestión operacional	3-42
3.5.	LA CONTRAINTELIGENCIA EN LAS OPERACIONES MULTINACIONALES	3-46
3.5.1.	Actividades de contrainteligencia en operaciones multinacionales	3-47
3.5.2.	ORGANIZACIÓN DE CONTRAINTELIGENCIA EN OPERACIONES MULTINACIONALES	3-48
3.5.3.	Recolección de información y reportes en las operaciones multinacionales	3-50
3.5.4.	Análisis de contrainteligencia en las operaciones multinacionales	3-50
3.6.	APOYOS DE CONTRAINTELIGENCIA	3-52
3.6.1.	Apoyo al proceso de selección y priorización de blancos	3-52
3.6.2.	Apoyo mediante la realización de estudios y recomendaciones de seguridad	3-52
3.6.3.	Apoyo a las actividades contra el narcotráfico	3-53
3.6.4.	Apoyo a las actividades de guerra electrónica	3-53
3.6.5.	Apoyo a la seguridad de las operaciones	3-54
3.6.6.	Apoyo a la contrapropaganda	3-55
3.6.7.	Apoyo a la contradecepción	3-56
3.6.8.	Apoyo contra el tráfico de armas de fuego, municiones y explosivos de uso privativo de las Fuerzas Militares	3-57

CAPÍTULO 4	RECOLECCIÓN DE INFORMACIÓN	4-1
4.1.	GENERALIDADES	4-2
4.2.	FUENTES PARA LA RECOLECCIÓN DE INFORMACIÓN DE CONTRAINTELIGENCIA	4-4
4.2.1.	Casual informal	4-4
4.2.2.	En desarrollo	4-5
4.2.3.	En control formal	4-6
4.3.	DEBRIEFING Y EVALUACIÓN	4-6
4.3.1.	<i>Debriefing</i> de contrainteligencia	4-6
4.3.2.	Evaluación de personal para obtención de información de contrainteligencia	4-11
4.4.	CONTROL DE INFORMACIÓN DE LA FUENTE	4-12
4.5.	GESTIÓN DE REQUERIMIENTOS DE CONTRAINTELIGENCIA	4-13
4.6.	REQUERIMIENTOS DE RECOLECCIÓN DE INFORMACIÓN PERMANENTES DE CONTRAINTELIGENCIA	4-15
4.7.	APOYO DE CONTRAINTELIGENCIA A EVALUACIONES DE AMENAZAS Y EVALUACIONES DE VULNERABILIDADES	4-16
CAPÍTULO 5	ANÁLISIS DE CONTRAINTELIGENCIA	5-1
5.1.	GENERALIDADES	5-2
5.2.	ANÁLISIS DE INFORMACIÓN	5-4
5.2.1.	Apreciaciones dinámicas	5-5
5.2.2.	Análisis de amenazas de contrainteligencia	5-5
5.3.	ANÁLISIS OPERACIONAL	5-8
5.3.1.	Identificación de anomalías, indicadores y patrones	5-10
5.3.2.	Perfilación de fuentes	5-10
5.4.	HERRAMIENTAS ANALÍTICAS	5-12
5.4.1.	Diagrama de eventos en el tiempo	5-12
5.4.2.	Matrices	5-14
5.4.3.	Diagrama de análisis de enlaces	5-19
5.5.	APOYO DE CONTRAINTELIGENCIA PARA LA PREPARACIÓN DE INTELIGENCIA DEL CAMPO DE COMBATE	5-29
5.5.1.	Planeamiento operacional	5-29
5.5.2.	Listas de blancos de CI	5-30

CAPÍTULO 6	SERVICIOS TÉCNICOS DE CONTRAINTELIGENCIA	6-1
6.1.	GENERALIDADES	6-2
6.2.	INTELIGENCIA DE FUENTES ABIERTAS (OSINT)	6-3
6.2.1.	Empleo de OSINT en los niveles de la guerra	6-4
6.2.2.	Ventajas de la OSINT	6-5
6.2.3.	Desventajas de la OSINT	6-6
6.2.4.	Explotación de la OSINT en apoyo a las actividades de contrainteligencia	6-6
6.3.	CONTRAMEDIDAS DE VIGILANCIA ELECTRÓNICA	6-8
6.3.1.	Examen de contramedidas de vigilancia electrónica	6-12
6.3.2.	Inspección de contramedidas de vigilancia electrónica	6-12
6.3.3.	Apoyo de contramedidas de vigilancia electrónica previas a la construcción	6-14
6.4.	IDENTIFICACIÓN MEDIANTE CARACTERÍSTICAS BIOMÉTRICAS	6-16
6.5.	APOYO DE PRUEBAS TÉCNICAS PSICOFISIOLÓGICAS DE VERACIDAD	6-17
6.5.1.	Exámenes psicofisiológicos de polígrafo	6-18
6.6.	INFORMÁTICA FORENSE	6-20
6.6.1.	Procedimiento para el manejo de datos digitales	6-21
6.6.2.	Ánalysis de datos digitales	6-23
CAPÍTULO 7	CIBERCONTRAINTTELIGENCIA	7-1
7.1.	GENERALIDADES	7-2
7.2.	PROPÓSITOS DE LA CIBERCONTRAINTTELIGENCIA	7-2
7.3.	LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERCONTRAINTTELIGENCIA	7-3
7.4.	CONTRIBUCIONES DE LA CIBERCONTRAINTTELIGENCIA A LAS OPERACIONES EN EL CIBERESPACIO	7-4
7.4.1.	Técnicas antiforenses	7-4
7.5.	OPERACIONES DE CIBERCONTRAINTTELIGENCIA	7-6
7.5.1.	Procedimiento de defensa activa	7-7
7.5.2.	Averiguaciones de intrusión en redes	7-13
7.6.	ACTIVIDADES INTERAGENCIALES DE CIBERCONTRAINTTELIGENCIA	7-15
7.7.	APOYO DE LA CIBERCONTRAINTTELIGENCIA AL ANÁLISIS Y LA PRODUCCIÓN DE CONTRAINTLIGENCIA	7-16
7.8.	CATEGORÍAS DE INCIDENTES EN LA RED	7-17
7.9.	INDICADORES DE INTERÉS CIBERNÉTICO	7-19

7.10. MANEJO DE DISPOSITIVOS COMPROMETIDOS EN UN INCIDENTE CIBERNÉTICO	7-21
7.11. OTROS ASPECTOS PARA TENER EN CUENTA EN LA RECOLECCIÓN DE INFORMACIÓN	7-23

ANEXO A	INFORME DE CONTRAINTELIGENCIA	A-1
ANEXO B	INFORME DE RECOLECCIÓN DE INFORMACIÓN	B-1
ANEXO C	INFORME DE RESULTADOS	C-1
ANEXO D	INFORME DE CIERRE	D-1
ANEXO E	INFORME ANÁLISIS DEFENSA ACTIVA	E-1

GLOSARIO

1.	ABREVIATURAS, SIGLAS Y ACRÓNIMOS	GLOSARIO-1
2.	TÉRMINOS	GLOSARIO-5

REFERENCIAS

REFERENCIAS-1

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

INTRODUCCIÓN

La constrainteligencia (CI) hace parte de las disciplinas de la función de conducción de la guerra (FCG) Inteligencia. Su objetivo es preservar los activos críticos del Ejército y contrarrestar la capacidad de recolección de información de las amenazas internas y externas. Los principios de constrainteligencia están contenidos en el MFE 2-0 y el MFRE 2-0.

La constrainteligencia opera transversalmente en las diferentes tareas ejecutadas por el Ejército para desarrollar el concepto operacional “operaciones terrestres unificadas” como principal aporte a las operaciones conjuntas dentro de la acción unificada.

Este manual describe las operaciones, acciones, actividades y procedimientos de constrainteligencia en relación con las funciones, competencias distintivas y objetivos de esta disciplina. Además, se convierte en la base de las técnicas de constrainteligencia y el fundamento doctrinal para los futuros cursos de capacitación en cuanto a las competencias distintivas y las funciones de la disciplina.

La principal audiencia del MCE 2-22.1 son los agentes, las secciones de inteligencia y constrainteligencia y el personal autorizado por la Ley 1621 de 2013, para manejar información reservada, de acuerdo con los niveles de clasificación contemplados en el artículo 2.2.3.6.2. del Decreto 1070 de 2015.

A continuación, se describe brevemente el contenido por capítulos de este manual. El capítulo 1 presenta los fundamentos, competencias distintivas de la CI en apoyo a los diferentes niveles de la guerra y la CI en las operaciones terrestres unificadas; el capítulo 2 describe las acciones de recolección de información de la amenaza y presenta las acciones de respuesta generadas por la CI; el capítulo 3 desarrolla las operaciones de constrainteligencia, sus procedimientos y apoyos; el capítulo 4 trata sobre la recolección de información realizada por el Ejér-

cito, el *debriefing*, los planes, los requerimientos y las fuentes; el capítulo 5 se enfoca en el análisis de CI y en las herramientas analíticas empleadas para su tratamiento; el capítulo 6 explica los servicios técnicos de constrainteligencia y su aporte a las operaciones militares. Finalmente, el capítulo 7 aborda la ciberconstrainteligencia y las actividades de recolección de información en el ciberespacio.

Los términos definidos se encuentran identificados en el cuerpo del texto con **cursiva** y **negrilla**, si su proponente es esta publicación, y se acompañan por un asterisco (*) en el glosario. Estos estarán incluidos en la próxima actualización del MFRE 1-02. Para las otras definiciones, el término va en *cursiva* y el número de la publicación proponente le sigue a la definición.

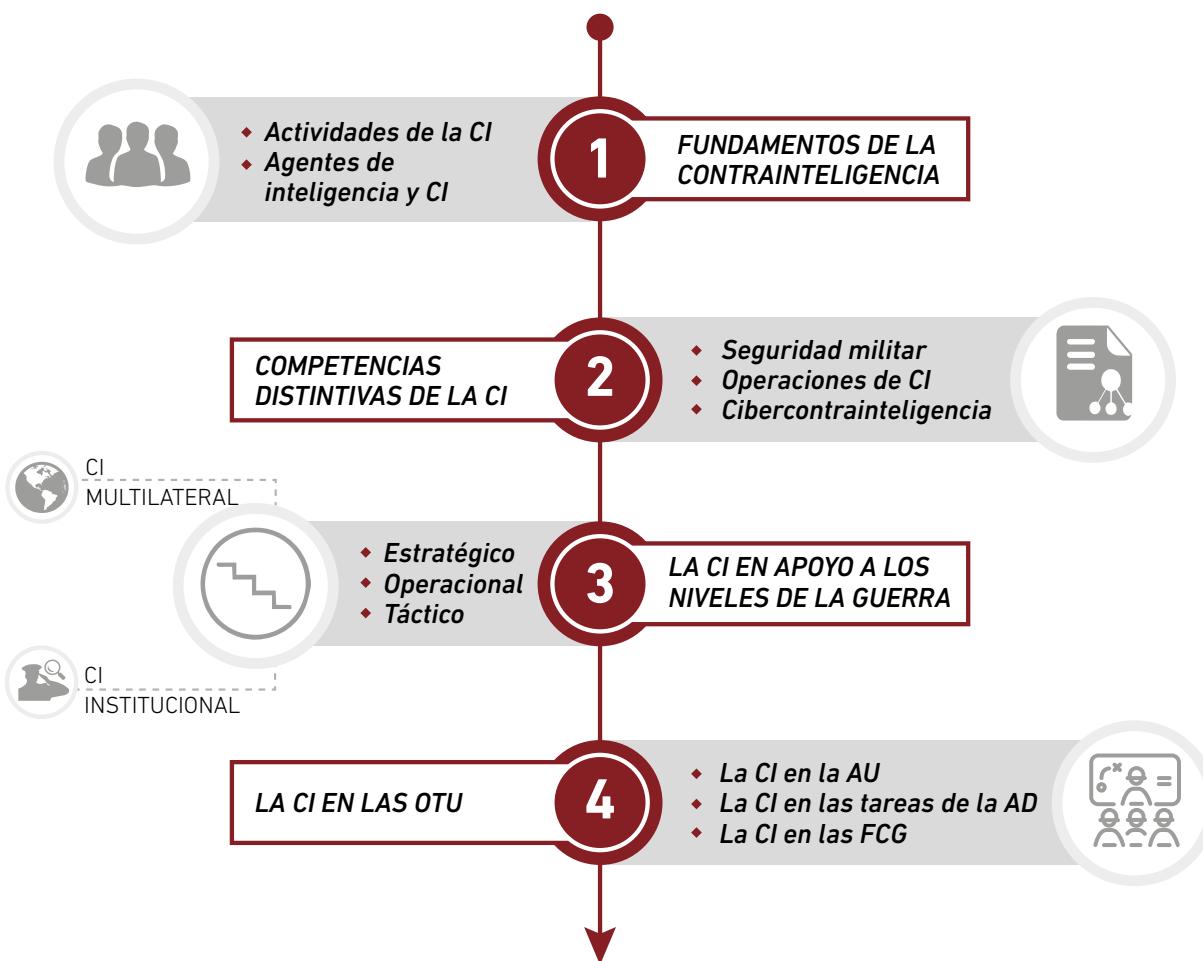
El proponente del MCE 2-22.1 es la Dirección de Producción, Organización y Equipamiento (DIPOE); por lo cual, los comentarios o recomendaciones al mismo deben hacerse llegar al correo electrónico dipoe@ejercito.mil.co

CAPÍTULO 1

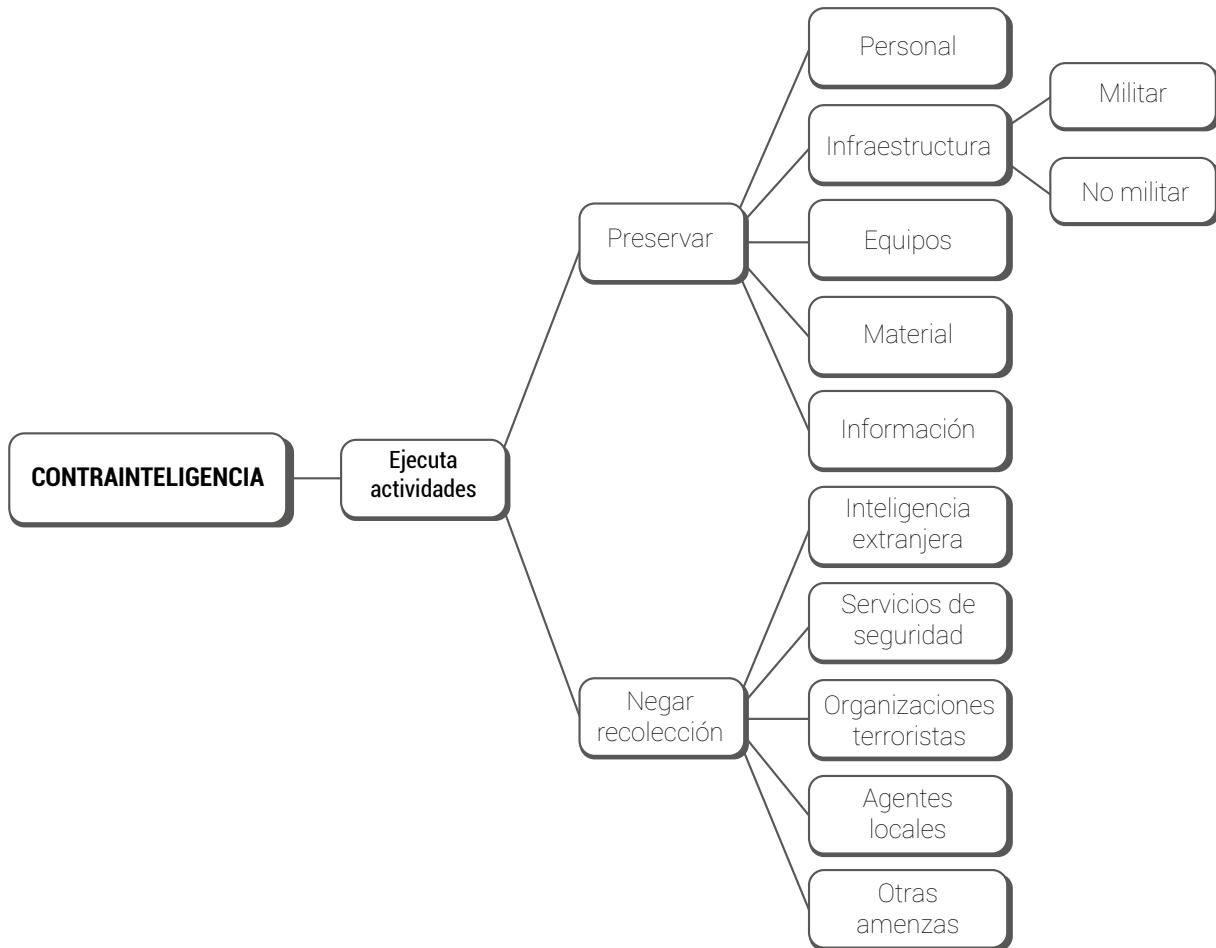
LA CONTRAINTELIGENCIA

“Estoy preocupado por la seguridad de nuestra gran nación; no tanto por una amenaza externa, sino por las fuerzas insidiosas que trabajan desde adentro”.

Douglas MacArthur



[1-1] La *contrainteligencia* (CI) es el conjunto de actividades destinadas a la preservación de personal, instalaciones, infraestructura, equipos, material e información que están encaminadas a identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar la recolección de información de la inteligencia extranjera y servicios de seguridad, las organizaciones terroristas, agentes locales y otras amenazas (MFE 2-0).



| Figura 1-1 | La contrainteligencia

[1-2] La constrainteligenzia es desarrollada por agentes capacitados y entrenados, que ejecutan actividades enfocadas a identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar la recolección de información de Inteligencia Extranjera y Servicios de Seguridad (FISS, por su sigla en inglés), organizaciones terroristas (OT), agentes locales y otras amenazas.

[1-3] Los líderes de constrainteligenzia deben propender, en la medida de sus capacidades y potestades, por la capacitación y reentrenamiento del personal bajo su mando, a fin de cumplir con la intención y el deber ser de las actividades que desarrolla el personal de agentes.

[1-4] La CI apoya las funciones de conducción de la guerra (FCG) mediante el desarrollo de operaciones, actividades, tareas, técnicas y procedimientos que se ejecutan de acuerdo con la necesidad operacional. Así, ejecutará, apoyará, intervendrá y/o coadyuvará de forma activa en la conducción de las diferentes tareas de las unidades del Ejército, con el propósito de alcanzar los objetivos establecidos para llegar al estado final deseado.

[1-5] Igualmente, la constrainteligenzia del Ejército analiza las actividades de recolección de información de la inteligencia de la amenaza que atenten contra la Fuerza (personal, instalaciones, información, entre otros). El análisis de CI incorpora la información recolectada por múltiples fuentes, como producto de las averiguaciones y las operaciones y la resultante de toda acción llevada a cabo en respuesta a las actividades de inteligencia de los adversarios. Con esto permite un análisis multidisciplinario que busca satisfacer los requerimientos de información de los comandantes.

[1-6] **La inteligencia extranjera es una organización de carácter secreto que recopila información reservada o clasificada.** La información obtenida tendrá nivel de clasificación ultrasecreto tal como se establece en el artículo 2.2.3.6.2 del Decreto 1070 del 2015, debido a que esta podría afectar hacia el exterior del país los intereses del Estado o las relaciones internacionales. Es posible que las actividades desarrolladas por los miembros de este tipo de organizaciones pongan en

CI

Constrainteligenzia

riesgo la integridad de la nación o a los asociados de la acción unificada (AU). Dependiendo del tipo de actividad realizada por el enemigo, podría afectar directamente los objetivos de nivel nacional o aquellos trazados por los asociados de la AU.

[1-7] Usualmente estas organizaciones son de carácter estatal o militar y sus actividades están reglamentadas y autorizadas por un gobierno extranjero, aunque también existen organizaciones de tipo clandestino. En cualquiera de los casos actúan y se entienden como *inteligencia extranjera*, ya que la información podría provenir o estar destinada a dichos servicios de inteligencia. Estas organizaciones tienen dos tipos de estructuras: una visible, que recolecta información de fuentes abiertas y hace análisis y actividades de carácter administrativo, y otra clandestina, encargada del manejo de fuentes y de información crítica.

[1-8] De igual forma se presentan los **servicios de seguridad** definidos como **organizaciones público-privadas que desarrollan actividades asociadas con la seguridad y/o la recolección de información**. Algunas de estas organizaciones son constituidas legalmente y prestan servicios de seguridad tradicionales (cámaras, sensores, seguridad física, entre otros). Sin embargo, existen servicios de seguridad clandestinos, y en ocasiones, ilegales, que tienen capacidad de recolectar información destinada a fines particulares y que podrían llegar a vulnerar la seguridad nacional o los intereses particulares de la AU.

AU | Acción unificada

[1-9] Un **agente local** es una **persona que posee acceso a información reservada o clasificada y puede entregar información de forma voluntaria o involuntaria**. Esta persona puede actuar individualmente o representar una organización gubernamental, no gubernamental, privada o al margen de la ley. La información que recolecta será empleada de acuerdo con las intenciones del enemigo, las cuales podrán indicar: la realización de actividades de espionaje, sabotaje, subversión y terrorismo, la extorsión o manipulación del personal para entrega o venta de información; afectación a la imagen Institucional por fuga de información a medios de comunicación, entre otras.

[1-10] Por su parte amenaza es cualquier combinación de actores, entidades o fuerzas que tienen la capacidad y la intención de afectar las fuerzas amigas, los intereses nacionales o la nación (MFRE 3-0). Es decir, la CI se enfrenta a un amplio rango de amenazas que pueden variar, mutar y desarrollar capacidades emergentes en un determinado ambiente operacional. Algunas de estas amenazas utilizan métodos y técnicas similares a los servicios de inteligencia para recolectar información y reclutar fuentes para el beneficio de una actividad criminal, como narcotráfico, corrupción, reclutamiento de menores de edad, extorsión, terrorismo, entre otros.

1.1. FUNDAMENTOS DE LA CONTRAINTELIGENCIA

[1-11] La CI recolecta información para proteger el personal, las instalaciones, el equipo, el material y la información asegurando la ventaja militar en las operaciones sobre los adversarios actuales y futuros. Al negar la capacidad de recolección de inteligencia del adversario, impidiéndole el conocimiento de los intereses y objetivos del Gobierno nacional, la CI apoya la defensa nacional, la seguridad pública y la seguridad nacional.

[1-12] La doctrina de CI se basa en los principios y fundamentos establecidos en las FCG Inteligencia y Protección, descritas en los manuales fundamentales y fundamentales de referencia 2-0 y 3-37, desde los cuales se originan los contenidos de este manual de campaña, que permiten la sincronía de actividades en pro del cumplimiento de las tareas del Ejército.

1.1.1. Actividades de la constrainteligenzia

[1-13] La constrainteligenzia dirige su atención o interés a aquellos factores que representen o se constituyan como un riesgo para el Ejército o para la nación anfitriona cuando se actúa en apoyo a una operación multinacional. Estos riesgos se determinan procesando la información recolectada de acciones de la inteligencia enemiga efectuadas por parte de FISS, OT y otras amenazas, las cuales requieren la aplicación

CI | Contrainteligencia

FCG | Función de conducción de la guerra

FISS | Inteligencia extranjera y servicios de seguridad

OT | Organizaciones terroristas

CI | Contrainteligencia

ACTIVIDADES DE LA CONTRAINTELIGENCIA

Prevenir

Identificar

Detectar

Disuadir

Interrumpir

Desinformar

Explotar

Contrarrestar

Neutralizar

de técnicas y procedimientos de la disciplina para alcanzar el propósito o intención trazada por el comando superior, de acuerdo con la actividad que en cada caso se requiera, así:

- Prevenir es la sincronización de medidas anticipadas necesarias para evitar la materialización de un suceso o acontecimiento adverso. La CI implementa técnicas y procedimientos para evitar que el enemigo pueda realizar actividades de recolección de información de inteligencia o cualquier otra de sus intenciones, contribuyendo a mitigar los riesgos de los activos críticos del Ejército.
- Identificar se refiere al reconocimiento de una persona, un hecho, una situación o un elemento sobre cualquiera de los cuales se tenía previa información. La recolección de información de CI y el análisis de CI permiten establecer personas u organizaciones, valiéndose del desarrollo de operaciones de contrainteligencia y de la verificación de bases de datos, con el fin de permitir el estudio detallado de la amenaza y de los cursos de acción necesarios para contrarrestarla.
- Detectar es revelar la existencia de una persona o una actividad de la cual no se tenía conocimiento previo. La CI permite hacer visibles las intenciones ocultas o secretas de personas, organizaciones o elementos que tengan el interés o la capacidad de afectar a la institución, a las fuerzas amigas o los intereses de la nación.
- Disuadir es inducir a alguien a cambiar de opinión o a desistir de un propósito. La CI desarrolla técnicas para subvertir el propósito inicial de la amenaza y lograr obtener la ventaja militar en donde anteriormente se vislumbraba un perjuicio actual o potencial.
- Interrumpir es cortar la continuidad de una acción enemiga o de sus comunicaciones. De acuerdo con la identificación de la amenaza y los riesgos que puede representar para la Fuerza, la disciplina de CI propenderá por obstaculizar el flujo de información entre la amenaza y el personal dentro de la Fuerza, así como sus sistemas de

comunicación, de igual forma, impedirá la persistencia de acciones nocivas para la institución.

- Desinformar se refiere a brindar información intencionalmente manipulada, alterada, falsa o incipiente, con fines específicos. Comprende un conjunto de actividades que sirven como contramedida para engañar o confundir al enemigo sobre los planes, intenciones o capacidades propias. Para desinformar se podrá recurrir a fuentes humanas o al manejo de la información dispuesta en el ciberespacio.
- *Explorar* es una tarea ofensiva que usualmente sigue a la conducción de un ataque exitoso y está diseñada para desorganizar al enemigo en profundidad (MFRE 3-90). En términos de inteligencia, la explotación se traduce en la toma de la ventaja militar obtenida gracias a la información recolectada en el desarrollo de una operación. La CI procura la identificación del enemigo y disminuye la capacidad de inteligencia extranjera y servicios de seguridad (FISS), organizaciones terroristas (OT), agentes locales y otras amenazas.
- Contrarrestar se refiere a disminuir o anular el efecto o la influencia de una actividad determinada mediante la ejecución de acciones de mitigación. La CI determina las técnicas y procedimientos que se van a emplear para compensar la acción del enemigo y sus alcances.
- *Neutralizar* se refiere una tarea táctica de la misión que tiene como resultado la incapacidad del personal o material del enemigo para interferir en una operación particular (MCE 3-90.1). En CI se podrá realizar suministrando información que conlleve a desarticular las redes de inteligencia enemiga. La neutralización inhibe la capacidad de CI del Ejército para identificar plenamente a todos los participantes y evaluar el daño causado a la seguridad nacional; por este motivo deberá efectuarse después la evaluación dada entre la oportunidad operacional y la continuidad de la operación de CI.

CI

Contrainteligencia

1.1.2. Agentes de inteligencia y contrainteligencia

[1-14] **Un agente en el ámbito de la inteligencia, es un oficial, suboficial, soldado o civil (dado de alta por el Ministerio de Defensa Nacional como auxiliar de inteligencia), quien se encuentra autorizado, capacitado y entrenado para desarrollar actividades de inteligencia o contrainteligencia.** Los agentes de CI tienen la misión de recolectar información de inteligencia extranjera y servicios de seguridad (FISS), organizaciones terroristas (OT), agentes locales y otras amenazas; su capacitación y reentrenamiento serán responsabilidad de los comandantes a todo nivel, en procura de mantener el desarrollo óptimo de las actividades de CI.

CI | Contrainteligencia

[1-15] Aunque las técnicas y procedimientos para recolectar información son similares entre la CI y la inteligencia, existen ciertas diferencias entre las actividades desempeñadas por los agentes de CI y aquellas efectuadas por los recolectores de inteligencia, las cuales se encuentran asociadas principalmente a la misionalidad, el objetivo y las tareas ordenadas. El empleo de agentes de CI en actividades de inteligencia afecta la capacidad del Ejército para proteger el personal, la información y las instalaciones (militares y no militares), debido a que se incumplen los principios de compartimentación, idoneidad y seguridad al exponer la identidad de los agentes de CI y sus capacidades, puesto que estos también operan en misiones enfocadas al personal de inteligencia de la misma Fuerza.

FCG | Función de conducción de la guerra

[1-16] El personal inmerso en actividades de contrainteligencia deberá tener el perfil de seguridad (credibilidad y confiabilidad) requerido para la disciplina; y el perfil profesional respaldado por la continua capacitación y entrenamiento, lo cual es distintivo de otras disciplinas de la FCG Inteligencia, obedeciendo a los principios de reserva legal, compartimentación y seguridad; para salvaguardar la identidad de los agentes y mantener la seguridad en las operaciones, debido a que los agentes podrían estar adelantando operaciones o actividades de CI contra personal que se desempeña en las otras disciplinas de la FCG Inteligencia.

INTELIGENCIA EXTRANJERA

Organización de carácter secreto que recolecta información reservada o clasificada (MCE 2-22.1).

SERVICIOS DE SEGURIDAD

Organizaciones público-privadas que desarrollan actividades asociadas con la seguridad y/o la recolección de información (MCE 2-22.1).

AGENTE LOCAL

Persona que posee acceso a información reservada o clasificada y puede entregar información de forma voluntaria o involuntaria (MCE 2-22.1).

AGENTE

En el ámbito de la inteligencia, es un oficial, suboficial, soldado o civil (dado de alta por el Ministerio de Defensa Nacional como auxiliar de inteligencia), quien se encuentra autorizado, capacitado y entrenado para desarrollar actividades de inteligencia o contrainteligencia (MCE 2-22.1).

COMPETENCIAS DISTINTIVAS DE LA CONTRAINTELIGENCIA

Seguridad militar

Operaciones de contrainteligencia

Cibercontrainteligencia

1.2. COMPETENCIAS DISTINTIVAS DE LA CONTRAINTELIGENCIA

[1-17] Las *competencias distintivas* se definen como una capacidad esencial y perdurable que un arma o una organización proporciona a las operaciones del Ejército (MFE 1-01). La contrainteligencia tiene tres competencias distintivas:

- 1) Seguridad militar.
- 2) Operaciones de contrainteligencia.
- 3) Cibercontrainteligencia (CCI)

SEGURIDAD MILITAR

Es la capacidad militar basada en el análisis y diagnóstico de amenazas, riesgos y vulnerabilidades relacionadas con la seguridad de personas, seguridad física, seguridad de la información y seguridad de la infraestructura crítica, dirigida a recomendar medidas activas y/o pasivas contra posibles acciones de una amenaza (MFRE 3-37).

OPERACIONES DE CONTRAINTELIGENCIA

Secuencia de tareas tácticas para la recolección de información sobre las acciones de inteligencia de la amenaza y los indicios de corrupción al interior de la Fuerza.

COMPETENCIAS DISTINTIVAS DE LA CONTRAINTELIGENCIA**CIBERCONTRAINTELIGENCIA**

Actividades desarrolladas en el ciberespacio para contrarrestar las acciones de la amenaza y apoyar la recolección de información de contrainteligencia.

| Figura 1-2 | Competencias distintivas de contrainteligencia

1.2.1. Seguridad militar

[1-18] La *seguridad militar* es la capacidad militar basada en el análisis y diagnóstico de amenazas, riesgos y vulnerabilidades relacionados con la seguridad de personas, seguridad física, seguridad de información y seguridad de la infraestructura crítica, dirigida a recomendar medidas activas y/o pasivas contra posibles acciones de una amenaza (MFRE 3-37).

[1-19] La seguridad militar busca generar condiciones de seguridad enfocadas en la preservación de la integridad, la credibilidad y la confiabilidad de los elementos que comprenden la Fuerza o los asociados de la AU (información, personas, material, instalaciones, entre otros). Esta competencia distintiva interactúa con la FCG Protección y apoya la recolección de información mediante el desarrollo de técnicas y procedimientos que tienen como fin suministrar informes de inteligencia y CI.

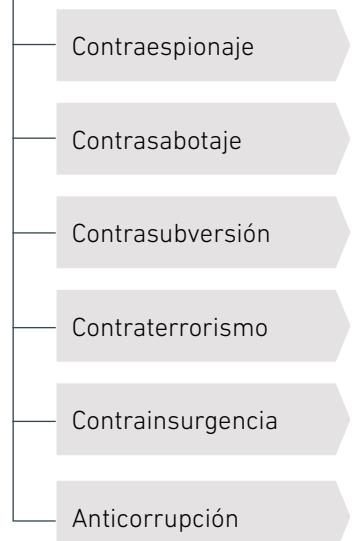
AU	Acción unificada
FCG	Función de conducción de la guerra
CI	Contrainteligencia

1.2.2. Operaciones de contrainteligencia

[1-20] Una *operación* es una secuencia de acciones tácticas con un propósito común o un tema unificador (MFE 1-01). Las **operaciones de contrainteligencia** se definen como la **secuencia de acciones tácticas para la recolección de información sobre las acciones de inteligencia de la amenaza y los indicios de corrupción al interior de la fuerza**. Una operación de contrainteligencia se configurará siempre y cuando se cumplan los parámetros establecidos en el procedimiento operacional de CI, y podrán clasificarse de la siguiente manera:

- Operaciones de contraespionaje.
- Operaciones de contrasabotaje.
- Operaciones de contrasubversión.
- Operaciones de contraterrorismo.
- Operaciones de contrainsurgencia.
- Operaciones anticorrupción.

OPERACIONES DE CONTRAINTELIGENCIA



[1-21] Las clases de operaciones descritas corresponderán a las acciones de respuesta de la CI a las acciones de la inteligencia de la amenaza, como se explica en el capítulo 3.

[1-22] Por otra parte, las actividades de cibercontrainteligencia (CCI) se pueden configurar en operaciones que pueden ser independientes o constituirse en un apoyo para cualquiera de las operaciones ya descritas. Las ***operaciones de cibercontra-inteligencia*** se definen como **acciones tácticas que permiten recolectar información de constrainteligencia, para identificar, analizar contrarrestar y neutralizar acciones de la amenaza en el ciberespacio**.

1.2.3. Cibercontrainteligencia

[1-23] La ***cibercontrainteligencia*** se define como las **actividades desarrolladas en el ciberespacio para contrarrestar las acciones de la amenaza y apoyar la recolección de información de constrainteligencia**. Ver el capítulo 7 para obtener información detallada acerca de esta competencia distintiva.

1.3. LA CONTRAINTELIGENCIA EN APOYO A LOS NIVELES DE LA GUERRA

CI

Contrainteligencia

[1-24] La CI es fundamental en todo el rango de operaciones militares (ROM), por ello podrá desarrollar sus funciones y competencias distintivas de acuerdo con la necesidad operacional. Los *niveles de la guerra* son un marco para definir y clarificar la relación entre los objetivos nacionales, el enfoque operacional y las tareas tácticas (MFE1-01). Los niveles de la guerra se correlacionan con niveles específicos de responsabilidad y tareas que comandantes y estado mayor/plana mayor deben cumplir, según les corresponda.

PMTD

Proceso militar para la toma de decisiones

[1-25] La CI apoyará con el desarrollo de actividades orientadas según el nivel de la guerra en el que se encuentren operando, a fin de brindarles a los tomadores de decisiones los elementos necesarios para el desarrollo del PMTD.

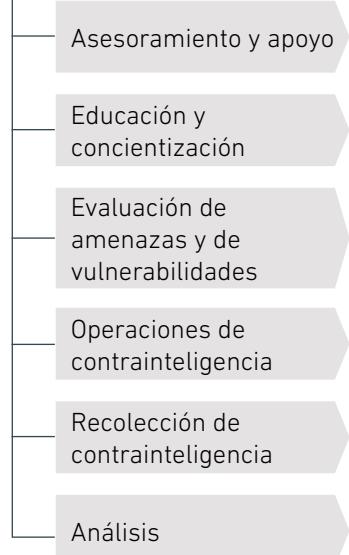
1.3.1. Nivel estratégico

[1-26] El *nivel estratégico* establece los objetivos nacionales, multinacionales y de teatro. El nivel estratégico de la guerra es principalmente del ámbito del liderazgo nacional y se expresa en la doctrina conjunta y las estrategias de seguridad, de defensa y militares (MFE 1-01). Las actividades de CI apoyan las operaciones conjuntas o multinacionales y las operaciones especiales que tengan impacto estratégico, teniendo en consideración y respetando la legislación de la nación anfitriona. A nivel estratégico, la CI desarrolla sus actividades en estricto cumplimiento del principio de compartimentación para afectar el conocimiento que FISS, OT u otras amenazas pretendan obtener con respecto a las operaciones y a la información recolectada. La contrainteligencia desarrolla, entre otras, las siguientes actividades:

- **Asesoramiento y apoyo:** Asesora a los comandantes, agentes de CI o unidades apoyadas sobre las políticas de seguridad aplicables a su nivel y proporciona información acerca de FISS, OT, agentes locales y otras amenazas que sirva para complementar los vacíos de información existentes; de igual forma, indica la manera adecuada en que se debe informar sobre la posible fijación de objetivos de la amenaza e incidentes de interés para la CI.
- **Educación y concientización:** Brinda orientación sobre las capacidades de FISS, OT, agentes locales y otras amenazas, para concientizar y educar al personal, como una medida para protegerlo de acciones de la amenaza, así como fuente de información para identificar, detectar y explotar anomalías, indicadores y patrones que representen un riesgo para la seguridad, lo cual permite iniciar averiguaciones de CI y fortalecer la aplicación de medidas de seguridad.
- **Evaluación de amenazas (EA) y evaluación de vulnerabilidades (EV):** Determina y evalúa la recolección de información y el análisis de datos de la amenaza para proporcionar al comandante, agencia o unidad apoyada la valoración de las medidas de protección y la apli-



ACTIVIDADES DE CONTRAINTELIGENCIA



EA	Evaluación de amenazas
EV	Evaluación de vulnerabilidades
CI	Contrainteligencia
AU	Acción unificada
FISS	Inteligencia extranjera y servicios de seguridad
OT	Organizaciones terroristas

ción de contramedidas adoptadas para contrarrestar las amenazas o vulnerabilidades actuales o potenciales presentes en el desarrollo de la operación. El propósito de la EA y la EV es plantear las medidas de eficacia (MEDEF) y las medidas de desempeño (MEDES) necesarias en cada caso, las cuales se actualizan y ajustan continuamente de acuerdo con las circunstancias y condiciones cambiantes del ambiente operacional. Esta actividad será desarrollada por las unidades de CI cuya misión sea la ejecución de las funciones de la competencia distintiva de seguridad militar.

- **Operaciones de contrainteligencia:** Explota y neutraliza las actividades de recolección de información de la amenaza dirigidas contra el Ejército o los asociados de la AU.
- **Recolección de contrainteligencia:** Identifica y detecta FISS, OT, agentes locales y otras amenazas dirigidas contra la Fuerza o los asociados de la acción unificada para proyectar y desarrollar medidas enfocadas a contrarrestar, disuadir, desinformar, explotar o neutralizar la capacidad de recolección de información del enemigo.
- **Análisis:** Determina, a partir de métodos de análisis, los posibles cursos de acción para los tomadores de decisiones que se encuentren asociados a escenarios en tiempo real o prospectivo, que permitan la protección y seguridad en las operaciones, con la intención de formular recomendaciones que contribuyan a seleccionar y ejecutar las acciones pertinentes para la mitigación del riesgo.

[1-27] En este nivel estratégico, la CI enfoca el desarrollo de sus actividades de acuerdo con las necesidades operacionales existentes, como se expone a continuación:

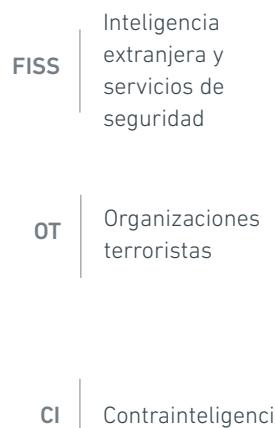
1.3.1.1. Contrainteligencia multilateral

[1-28] La **contrainteligencia multilateral** es una función de contrainteligencia que **direcciona y desarrolla sus actividades para apoyar la seguridad nacional, defensa nacional y seguridad pública**. Dado que las amenazas actuales y futuras

se encuentran asociadas a la afectación (o la eventual afectación) en seguridad contra varios Estados o que repercuten negativamente en las relaciones entre estos, la CI multilateral enfoca su recolección de información en las redes de inteligencia extranjeras, las redes criminales transnacionales, las OT internacionales, agencias de inteligencia externas y los servicios de seguridad extranjeros. Así mismo, busca recolectar información acerca de acciones, planes o intenciones de FISS, OT u otras amenazas, sobre las cuales se sospeche o se generen indicios de actividades de incursión en territorio colombiano, y que impliquen un riesgo para la seguridad nacional, al conllevar una afectación social, económica, política, militar o cualquier otra que perjudique a la nación.

[1-29] La recolección de información incluye la verificación de incidentes en zonas de fronteras y el despliegue de agentes de CI a las áreas que sean requeridas, a fin de adelantar las actividades de CI. Esto permite prevenir, identificar, detectar, disuadir, interrumpir, desinformar, explotar, contrarrestar o neutralizar cualquier eventual amenaza. Esta no se limita a un espacio geográfico o territorial específico, sino que se debe entender en un amplio espectro en el que confluyen agentes, eventos, incidentes, elementos físicos o acciones en el ciberespacio que afecten a la nación y requieran una acción de respuesta por parte de la CI del Ejército. El éxito de la labor dependerá, en gran medida, del nivel de intercambio de información producto de la coordinación con otras agencias de inteligencia nacionales y extranjeras con las cuales haya objetivos comunes; y con las entidades gubernamentales o no gubernamentales que representen una autoridad en materia fronteriza.

[1-30] Esta función de CI dirige sus esfuerzos a promover ambientes de seguridad hemisférica que articulen iniciativas nacionales en respuesta a amenazas multiescalares de carácter regular o híbrido.



OPERACIONES DE CONTRAINTELIGENCIA

Secuencia de acciones tácticas para la recolección de información sobre las acciones de inteligencia de la amenaza y los indicios de corrupción al interior de la fuerza (MCE 2-22.1).

OPERACIONES DE CIBERCONTRAINTTELIGENCIA

Acciones tácticas que permiten recolectar información de contrainteligencia, para identificar, analizar contrarrestar y neutralizar acciones de la amenaza en el ciberespacio (MCE 2-22.1).

CIBERCONTRAINTTELIGENCIA

Actividades desarrolladas en el ciberespacio para contrarrestar las acciones de la amenaza y apoyar la recolección de información de contrainteligencia (MCE 2-22.1).

CONTRAINTTELIGENCIA MULTILATERAL

Función de contrainteligencia que dirige y desarrolla sus actividades para apoyar la seguridad nacional, defensa nacional y seguridad pública (MCE 2-22.1).

CONTRAINTTELIGENCIA INSTITUCIONAL

Función de contrainteligencia que busca identificar y contrarrestar las acciones de corrupción al interior de la Fuerza (MCE 2-22.1).

1.3.1.1.1. Contribución de la constrainteligenzia multilateral a las tareas de apoyar la seguridad nacional, apoyar la defensa nacional y apoyar la seguridad pública

[1-31] A continuación se presentan las tareas descritas en el MFE 2-0 y el MFRE 2-0 sobre la FCG Inteligencia, alineadas con conceptos doctrinales establecidos en el MFRE 3-0 *Operaciones*, seguidos por los eventos o manifestaciones que pueden presentarse en torno a las actividades propuestas por el enemigo o por la amenaza para el cumplimiento de sus objetivos, las cuales requieren ser objeto de averiguaciones y operaciones de CI, donde se empleen todas las técnicas y procedimientos necesarios que permitan, según el enfoque requerido por el comando superior, proteger y resguardar al Ejército y a la nación de intenciones, planes o acciones enemigas.

Apoyar la seguridad nacional

[1-32] La *seguridad nacional* se define como el esfuerzo nacional concertado para prevenir los ataques terroristas, reducir las vulnerabilidades a estos, atender desastres naturales y otras emergencias (MFRE 3-0).

[1-33] Estas son algunas actividades de la amenaza que pueden afectar la seguridad nacional y que son de interés para la constrainteligenzia multilateral.

- Actividades de subversión que afecten la seguridad nacional.
 - Manifestaciones que tengan como objetivo o pretendan subvertir a un grupo de personas con el fin de reclutarlos para hacer parte de organizaciones armadas ilegales o se empleen para el adoctrinamiento de personal, incitándolo a actuar de forma violenta para oponerse o derrocar a un gobierno democráticamente establecido bajo intereses de otro Estado o de una organización transnacional.

FCG	Función de conducción de la guerra
CI	Constrainteligenzia

- Participación o influencia de personas en insurrecciones o rebeliones.
 - Creación de organizaciones para suplantar al gobierno o a sus instituciones legalmente constituidas para desestabilizar una región o país.
 - Cualquier organización o agente que ayude, colabore y/o promueva a grupos ilegales o alzados en armas, que se encuentren en contra de los intereses del Estado.
- Actividades de espionaje que afecten la seguridad nacional:
 - Acceder a información de seguridad nacional, incluyendo bocetos, fotografías, planos, mapas, modelos, documentos, textos o cualquier otro.
 - Recolectar información acerca de la ubicación y funcionamiento de las infraestructuras críticas de la nación.
 - Entrar, sobrevolar u obtener información sobre instalaciones de seguridad nacional, bases militares, material estratégico, buques, aeronaves (o cualquier lugar designado como de interés nacional) para efectuar acciones en su contra.
 - Copiar, tomar, obtener o generar información referente a la seguridad nacional, incluyendo bocetos, fotografías, planos, mapas, modelos, documentos, textos o cualquier otro, sobre activos estratégicos del Estado.
 - Fotografiar, hacer grabaciones de video, dibujar, georreferenciar o crear una representación gráfica de instalaciones, equipos militares o navales vitales para las operaciones.
 - Obtener información de las redes o agentes de inteligencia y CI de la nación.

- Acceder a cualquier información de comunicaciones clasificada, incluidos códigos, cifrados, sistemas criptográficos o sistemas de inteligencia de señales.
 - Pretender entrar, comunicarse o tener contacto en una instalación diplomática colombiana en el extranjero, incluyendo embajadas o consulados, sin que se cuente con previo aviso o permiso.
- Actividades de sedición que afecten la seguridad nacional:
- Incitar, ayudar o comprometerse a cualquier acto hostil provocado o dirigido por extranjeros, que busquen generar actos contrarios a los intereses nacionales del país.
 - Imprimir, publicar, editar, emitir, circular, vender, distribuir o exhibir públicamente cualquier material escrito o audiovisual que defienda, aconseje o enseñe la necesidad o conveniencia de derrocar o destruir cualquier Estado, territorio, distrito, posesión, país u otras subdivisiones políticas, con la intención de afectar el Estado de derecho.
- Actividades de sabotaje que afecten la seguridad nacional:
- Dañar o destruir cualquier material de guerra con el propósito de obstruir o perjudicar la capacidad de defensa nacional.
 - Interrumpir intencionalmente el servicio o funcionamiento de cualquier infraestructura crítica.
 - Producir o influir en la producción de cualquier material de guerra, para que se elabore de manera defectuosa, con la intención de perjudicar, obstruir o interferir las operaciones militares o de inteligencia.
 - Apoyar, ayudar, colaborar o llevar a cabo cualquier ataque utilizando el espectro electromagnético (EEM) o el ciberespacio.

- Actividades de terrorismo que afecten la seguridad nacional:
 - Participar en conductas contrarias a las leyes penales nacionales que trasciendan las fronteras e involucren actos que vulneren los derechos humanos.
 - Fabricar artefactos explosivos o armas no convencionales con fines terroristas.
 - Usar armas de fuego o cualquier tipo de material bélico con el fin de generar terror entre la población civil.
 - Comunicar o transmitir por medios audiovisuales o escritos, mensajes que alteren la tranquilidad de la población colombiana.
 - Alterar el orden público mediante acciones terroristas.
 - Proporcionar o recaudar fondos con la intención de que se utilicen, o con el conocimiento de que se utilizarán, en su totalidad o en parte, para llevar a cabo cualquier acto terrorista destinado a favorecer intereses de otros países, agencias o personas.

CI | Contrainteligencia

[1-34] De igual forma, la CI emplea fuentes y agentes para ejecutar la recolección de información con el fin de identificar las acciones de la amenaza que afectan la seguridad nacional.

[1-35] La recolección de información de CI estará encamionada a:

- Identificar organizaciones de delincuencia organizada transnacional (DOT)
- Identificar y localizar finanzas ilícitas en zonas fronterizas (contrabando, hurto de hidrocarburos, etc.).
- Detectar e identificar redes de migración irregular.
- Detectar y localizar redes de tráfico de material de guerra.
- Detectar actividades de espionaje en zonas fronterizas.

- Identificar y detectar acciones, planes o intenciones de organizaciones terroristas transnacionales o de otras organizaciones internacionales consideradas amenazas, acerca de posibles incursiones en territorio colombiano.

[1-36] Las actividades anteriormente descritas se llevan a cabo con el fin de orientar tanto la toma de decisiones por medio de los informes de constrainteligenzia dirigidos al comandante del Ejército, como la toma de decisiones políticas a través de la inteligencia que se produce y se entrega a la Junta de Inteligencia Conjunta (JIC), que a su vez, genera los análisis de inteligencia y constrainteligenzia requeridos por el Consejo de Seguridad Nacional, que es el máximo organismo asesor del presidente de la República, en asuntos de seguridad nacional.

Apoyar la defensa nacional

[1-37] La *defensa nacional* se define como la protección de la soberanía, el territorio, la población nacional y la infraestructura de defensa crítica de Colombia contra las amenazas externas y la agresión u otras amenazas según las indicaciones del presidente de la República (MFRE 3-0).

[1-38] Las siguientes son algunas acciones de la amenaza que pueden afectar la defensa nacional y que son objetivo para la CI multilateral:

- Incursión de personas, grupos o células de inteligencia extranjera al territorio colombiano.
- Propagación de ideologías extremistas en territorio colombiano.
- Desarrollo de planes terroristas que intenten afectar las infraestructuras críticas de la nación.
- Desarrollo de actividades de cualquier tipo de espionaje por parte de organizaciones de inteligencia extranjera.

CI

Constrainteligenzia

[1-39] Las actividades que realiza la contrainteligencia multilateral en apoyo a la defensa nacional, sin que sean las únicas, podrán ser las siguientes:

- Identificación de actores armados o no armados que puedan llegar a desestabilizar el Estado de derecho o una parte de este.
- Anticipación de las acciones de las amenazas externas que afecten la defensa nacional.
- Recomendar medidas de defensa nacional a partir del conocimiento prevalente de las amenazas, mediante la entrega de informes de CI.
- Identificar y contrarrestar los factores de inestabilidad externos o internos con relación a zonas fronterizas mediante la recomendación de cursos de acción destinados a contrarrestar amenazas actuales y potenciales.
- Proporcionar al comandante militar o a la autoridad del gobierno nacional que lo requiera, el conocimiento prevalente de las amenazas a partir de la inteligencia recolectada por averiguaciones u operaciones de CI.
- Coordinar con autoridades gubernamentales y no gubernamentales con previa autorización del comando superior, el intercambio de información para refinar la inteligencia disponible.
- Degradar la capacidad de recolección de información de las redes de inteligencia externas sobre los intereses nacionales.

Apoyar la seguridad pública

[1-40] La *seguridad pública* se define como las actividades de prevención, detección y neutralización frente a amenazas de crimen organizado y delitos nacionales, transnacionales e internacionales, que atenten contra las condiciones de bienestar de la población civil, la prosperidad de las co-

munidades, la infraestructura y servicios asociados al Estado incluyendo los recursos naturales (MFRE 3-0).

[1-41] La constrainteligenzia ejecuta actividades de recolección de información en apoyo a la seguridad pública, en cumplimiento a los requerimientos y las prioridades establecidas en el Plan Nacional de Inteligencia, elaborado y emitido por la JIC, donde se asignan responsabilidades sobre la identificación y detección de la acción del crimen organizado nacional (grupos armados ilegales, guerrillas, grupos insurgentes, organizaciones terroristas locales, etc.) que afecten:

- Al Ejército Nacional.
- La infraestructura crítica de Colombia o de los asociados de la AU.
- Los recursos naturales.
- El bienestar de la población civil colombiana o de la nación anfitriona.
- Las condiciones de seguridad regionales o hemisféricas.

[1-42] Estos son algunos de los indicadores que pueden afectar la seguridad pública:

- Cuando un grupo de personas se organiza para cometer delitos de genocidio, desaparición forzada de personas, tortura, desplazamiento forzado, homicidio, terrorismo, narcotráfico, secuestro o extorsión para organizar, promover, armar o financiar grupos armados al margen de la ley.
- Amenazas difundidas por cualquier medio a una población, con el propósito de causar zozobra o terror.
- Reclutar, instigar o amenazar a la población para llevarla a ejecutar actividades de narcotráfico.
- Incitar a cometer delitos a otras personas por medio de coacción o amenazas.

JIC | Junta de inteligencia conjunta

AU | Acción unificada

- Incitar al personal de la Fuerza Pública o a los organismos de seguridad del Estado a desertar, a abandonar el puesto o el servicio o a poner en práctica cualquier acto preparatorio para este fin.
- Destruir ecosistemas protegidos.
- Utilizar el subsuelo o los recursos naturales para actividades ilegales, como minería ilegal, desvío de cauces de ríos, plantación de cultivos ilícitos, comercialización ilegal de animales, entre otros.

1.3.2. Nivel operacional

CI	Contrainteligencia
AO	Área de operaciones
FISS	Inteligencia extranjera y servicios de seguridad
OT	Organizaciones terroristas

[1-43] La CI a este nivel apoya con operaciones en un teatro específico, enfocándose en las actividades de respuesta de la CI que impidan recolectar información por parte de la amenaza y en aquellas que busquen contribuir a la protección del riesgo de infiltración o penetración por parte de la amenaza.

[1-44] Aunque en el nivel operacional la CI tiene una misión vital para contrarrestar la amenaza, sobre una base de actividades específicas se le puede encomendar la tarea de apoyar en determinadas operaciones militares cuando el tamaño, la escala y el alcance de esta exceda la capacidad proporcionada inicialmente por las unidades ubicadas en el teatro de operaciones; esto, con el fin de apoyar adecuadamente en el AO.

[1-45] Cuando sea necesario, las diferentes unidades de CI pueden tener la tarea de respaldar las operaciones estratégicas de esta disciplina. En este nivel, generalmente, se realizarán las siguientes actividades:

- **Asesoramiento y apoyo:** Asesorar a los comandantes, agentes de CI o unidades apoyadas en lo relativo a políticas de seguridad, proporcionando información de interés relacionada con FISS, OT, agentes locales y otras amenazas que sirvan para identificar acciones de la amenaza que lleven a ser informadas de manera oportuna, facilitando el desarrollo de actividades de CI.

- **Educación y concientización:** Informar al personal de la Fuerza, con fines de concientización y educación, sobre las actividades desarrolladas por parte de FISS, OT, agentes locales y otras amenazas. Esta es una medida de prevención que alerta sobre los indicadores observados en incidentes de CI previos que permiten apoyar en la mitigación de los riesgos producidos por la amenaza.
- **Evaluación de amenazas (EA) y evaluación de vulnerabilidades (EV):** Desarrollar y proporcionar los insumos de los análisis de CI y diagnósticos de seguridad realizados, que permitan al comandante, agencia o unidad apoyada replantear y fortalecer las medidas adoptadas para proteger el personal, el material, el equipo, la información y las operaciones. Esta actividad será desarrollada por las unidades de CI cuya misión sea la ejecución de las funciones de la competencia distintiva de seguridad militar.
- **Operaciones de contrainteligencia:** Explotar y neutralizar las actividades de recolección de la amenaza dirigidas a la Fuerza o a la nación.
- **Recolección de contrainteligencia:** Identificar y detectar FISS, OT, agentes locales y otras amenazas dirigidas a la nación o a la fuerza, con el propósito de realizar actividades que permitan contrarrestar, disuadir, desinformar, explotar o neutralizar la capacidad de recolección de información del enemigo.
- **Análisis:** Ejecutar adecuadamente el tratamiento de la información para proporcionar al comandante, unidad o agencia apoyada informes de CI que sirvan para planear operaciones y establecer las actividades de seguridad pertinentes para la protección de la nación y de la Fuerza.

[1-46] Las actividades, funciones y competencias distintivas de CI deben apoyar las tareas de la acción decisiva (AD) en un ambiente volátil, incierto, complejo o ambiguo (VICA), para responder a los *elementos esenciales de información de las propias tropas* (EEIPT), los cuales se definen como aspectos críticos de la operación de las propias tropas que de ser conocidos por el enemigo comprometerían, llevarían al fracaso

FISS	Inteligencia extranjera y servicios de seguridad
OT	Organizaciones terroristas
CI	Contrainteligencia

o limitarían el éxito de la operación; por lo tanto, deben ser protegidos de la detección por parte de este (MFRE 2-0).

1.3.3. Nivel táctico

[1-47] El *nivel táctico* hace referencia a la conducción de las acciones, batallas, combates y otras tareas tácticas para lograr los objetivos militares asignados a unidades tácticas o fuerzas de tarea (MFE 1-01). Los medios de recolección de información (MRI) de CI disponibles en la Fuerza para el cumplimiento de tareas del Ejército en este nivel, centran sus esfuerzos en la recolección de información de la inteligencia de la amenaza que atenten contra la Fuerza (personal, instalaciones, información, entre otros); de esta forma, vela por su resguardo y protección. El apoyo constante a las actividades del Ejército a nivel táctico permite que se obtengan logros significativos y posibilita el planeamiento con base en inteligencia debidamente procesada y analizada. Así, se deben cumplir, entre otras, las siguientes actividades:

CI	Contrainteligencia
FISS	Inteligencia extranjera y servicios de seguridad
OT	Organizaciones terroristas

- **Asesoramiento y apoyo:** Asesorar a los comandantes, agentes de CI, unidades o agencias apoyadas sobre las políticas de seguridad existentes y proporcionarles información acerca de las unidades de CI que poseen las capacidades para identificar FISS, OT, agentes locales y otras amenazas, así como sus métodos o técnicas para recolectar información. Esto se hace con el fin de que puedan solicitar apoyos con base en información e indicios sólidos que permitan adelantar averiguaciones y operaciones de CI.
- **Educación y concientización:** Consiste en permitir, por medio de informes y socializaciones, el conocimiento acerca de las acciones de inteligencia enemiga adelantadas por FISS, OT, agentes locales y otras amenazas, propendiendo por la concientización y educación del personal, de forma que permita generar indicios sobre posibles actividades del enemigo dentro de la Fuerza.

- **Evaluación de amenazas (EA) y evaluación de vulnerabilidades (EV):** Consiste en recopilar y analizar los datos obtenidos acerca de FISS, OT y otras amenazas que hayan afectado o puedan afectar una unidad, instalación, operación o actividad específica. De esta forma es posible proporcionar al comandante apoyado el conocimiento sobre la postura de protección y seguridad necesaria para formular las medidas requeridas con el fin superar las deficiencias o vulnerabilidades halladas. Esta es una actividad propia de la competencia distintiva de seguridad militar.
- **Operaciones de constrainteligencia:** Consisten en identificar los posibles indicadores o incidentes de CI, para iniciar objetivamente operaciones o averiguaciones de CI.
- **Recolección de constrainteligencia:** Consiste en identificar y detectar las actividades de recolección de información adelantadas por FISS, OT, agentes locales y otras amenazas, que se encuentren dirigidas a las unidades desplegadas en el nivel táctico, para lograr el diseño y aplicación de medidas tendientes a contrarrestar, disuadir, desinformar, explotar o neutralizar las acciones de inteligencia del enemigo.
- **Análisis:** Consiste en ejecutar la recolección de información acerca de las actividades de inteligencia de la amenaza. Esto permite efectuar un análisis inicial de dicha información, para planear y ejecutar las medidas necesarias para garantizar la protección y seguridad de los activos del Ejército.

[1-48] En los niveles operacional y táctico se encuentra el desarrollo de actividades de CI que permiten apoyar los procesos de transparencia adelantados en las unidades de los estados mayores de ejército (generador de fuerza y generador de combate), lo cual contribuye a la conservación de la buena imagen institucional.



1.3.3.1. Constrainteligenzia institucional

[1-49] La **constrainteligenzia institucional** es una función de constrainteligenzia que busca identificar y contrarrestar las acciones de corrupción al interior de la Fuerza, en lo relacionado con las amenazas generadas por las acciones de inteligencia del enemigo, que se encuentren destinadas a personal, infraestructura militar y no militar, información y equipos del Ejército.

CI | Constrainteligenzia

[1-50] La actuación de la CI en apoyo a los procesos administrativos del Ejército se manifiesta en actividades como la detección de redes de tráfico de influencias, corrupción administrativa, actuaciones irregulares en contratación, tráfico de medicamentos, desviación o malversación de recursos, manejo inadecuado de plataformas tecnológicas de la institución, tráfico de repuestos, tráfico de hidrocarburos y otras fenomenologías que interfieren en la efectividad de las actividades del Ejército.

[1-51] En lo referente a los procesos operacionales del Ejército, la CI adelanta sus actividades enfocando sus esfuerzos a las modalidades de tráfico de material de guerra, municiones y/o explosivos de uso privativo de las Fuerzas Militares, tráfico de información, tráfico de intendencia, casos de suplantación, penetración o infiltración a la Fuerza y otros que pongan o puedan poner en riesgo la integridad del personal que desarrolla las operaciones o reduzca las posibilidades de éxito operacional de una acción militar.

1.4. LA CONTRAINTELIGENCIA EN LAS OPERACIONES TERRESTRES UNIFICADAS

[1-52] La CI apoya el concepto operacional del Ejército operaciones terrestres unificadas (OTU) por medio de la ejecución de operaciones, actividades, funciones, técnicas y procedimientos, de acuerdo con las necesidades y requerimientos exigidos en la ejecución de la acción decisiva (AD). Esto requiere una capacidad de conducción durante la ejecución simultánea de tareas ofensivas, defensivas, de estabilidad o

de apoyo a la defensa a la autoridad civil, para alcanzar una sincronización del conocimiento prevalente de la inteligencia de la amenaza. De esta forma se busca ganar ventaja sobre el adversario, entendiendo sus intenciones y planes, planteando las acciones necesarias para resguardar a la Fuerza y privándoles el acceso a la información crítica con la cual podrían operar.

1.4.1. La constrainteligenzia en la acción unificada

[1-53] La constrainteligenzia apoya a los asociados de la AU mediante el desarrollo de tareas descritas en la FCG Inteligencia (ver el MFRE 2-0) apalancadas en los tres elementos que construyen la unión de esfuerzos de inteligencia: comunidad de inteligencia conjunta, arquitectura de inteligencia y profesionales de inteligencia. Lo anterior, guiado por la filosofía y la FCG Mando tipo misión, para que, de esta forma, se compaginen los insumos de inteligencia producto de las actividades de cooperación en la recolección de información obtenida por entidades públicas y privadas, en concordancia con la legislación vigente. Así mismo, se ayuda a las investigaciones judiciales, de acuerdo con las competencias y la protección legal que establece la legislación colombiana.

[1-54] La constrainteligenzia apoya la seguridad pública, la seguridad nacional y la defensa nacional. Esto se efectúa mediante la ejecución de actividades enfocadas a identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar las amenazas vinculadas con amenazas exteriores, crimen organizado (delitos nacionales, transnacionales e internacionales) o terrorismo, que atenten contra las condiciones de bienestar de la población civil y sus derechos inherentes, la prosperidad de las comunidades y la infraestructura crítica (militar y no militar) del Estado, incluyendo sus activos estratégicos y sus recursos naturales.

[1-55] Estas son algunas de las actividades con las que la CI, apoya la AU:

AU	Acción unificada
FCG	Función de conducción de la guerra

CI	Constrainteligenzia
----	---------------------

- La *cooperación en seguridad* es toda interacción entre el Ministerio de Defensa Nacional y los organismos de defensa extranjeros, que tiene como objetivo crear relaciones que promueven intereses específicos en materia de defensa y seguridad, con el fin de desarrollar capacidades militares aliadas para las operaciones de defensa mutua y multinacional (MFRE 3-0). La constrainteligenzia apoya esta actividad mediante la aplicación de sus capacidades, enfocadas tanto a la recolección de información como a la seguridad y protección de activos, permitiendo con ello la correcta articulación de la capacidad militar, que repercuta positivamente en el desarrollo de operaciones militares efectivas.
- La *defensa interna en el extranjero* (FID) es la participación de las agencias civiles y militares de un gobierno, en cualquiera de los programas de acción adoptados por otro gobierno o por otra organización designada, para liberar y proteger su sociedad de la subversión, la anarquía, la insurgencia, el terrorismo y otras amenazas a su seguridad (MFRE 3-0). La CI podrá desplegarse en apoyo a un plan de recolección de información en el extranjero con el fin de proteger los intereses de los asociados de la AU.

CI	Contrainteligenzia
AU	Acción unificada

[1-56] Así mismo, la CI apoya la seguridad pública, la seguridad nacional y la defensa nacional mediante la ejecución de actividades de CI frente a amenazas de crimen organizado, delitos nacionales, transnacionales e internacionales y terrorismo que atenten contra las condiciones de bienestar de la población civil, la prosperidad de las comunidades, la infraestructura y los servicios asociados del Estado, incluyendo los recursos naturales.

1.4.2. La constrainteligenzia en las tareas de la acción decisiva

[1-57] La constrainteligenzia cumple diversas tareas dentro la *acción decisiva*, la cual se define como la combinación continua y simultánea de tareas ofensivas, defensivas, de estabili-

dad o de apoyo de la defensa a la autoridad civil (MFRE 3-0). Mediante la acción decisiva es posible materializar las intenciones y proyecciones planteadas por la Fuerza, que permitan la consolidación del estado final deseado.

1.4.2.1. Tareas ofensivas

[1-58] Una *tarea ofensiva* es una tarea conducida para derrotar y destruir fuerzas enemigas, capturar terreno, recursos y centros poblados (MFRE 3-0). La CI apoya las tareas ofensivas mediante actividades de explotación, disuasión, desinformación y neutralización de las redes de inteligencia de la amenaza, al igual que con la ejecución de la competencia distintiva de cibercontrainteligencia, cuyos propósitos se encaminan a proporcionar inteligencia, que permita la materialización de las intenciones del comandante en el área de operaciones, transformando la acción enemiga en líneas de inteligencia accionables que impacten negativamente a la amenaza, al minimizar las capacidades de recolección de información y negar el desarrollo de acciones por parte de una amenaza dentro de la Fuerza; así mismo, emplea la información obtenida para recomendar los cursos de acción a los tomadores de decisiones durante el proceso militar para la toma de decisiones (PMTD) y el proceso de selección y priorización de blancos (PSPB) que le impliquen los más altos niveles de sorpresa y efectividad para la obtención del estado final deseado y que permitan, a su vez, la detección de las vulnerabilidades o debilidades explotables como acción de respaldo para la continuidad de las operaciones.

CI

Contrainteligencia

1.4.2.2. Tareas defensivas

[1-59] Una *tarea defensiva* es una tarea conducida para derrotar un ataque enemigo, ganar tiempo, economizar fuerzas y desarrollar condiciones favorables para tareas ofensivas o de estabilidad (MFRE 3-0). La CI apoya con tareas de protección mediante la competencia distintiva de la seguridad militar y sus funciones, las cuales tienen como fin proteger a las personas, la información, las instalaciones e infraestructura

crítica (militar y no militar), así como identificar los riesgos y amenazas presentes o potenciales en la Fuerza, generando con ello medidas activas y pasivas de seguridad tendientes a prevenir, detectar, minimizar o contrarrestar las proyecciones de la amenaza, permitiendo la conservación de condiciones favorables necesarias para la continuidad del desarrollo de las tareas ofensivas del Ejército, al preservar el estado mínimo y óptimo de los activos críticos del Ejército para el despliegue de las capacidades militares, de acuerdo con la necesidad operacional.

1.4.2.3. Tareas de estabilidad

CI	Contrainteligencia
AU	Acción unificada

[1-60] La *estabilidad* es la tarea que se conduce dentro o fuera del territorio nacional, en coordinación con otros instrumentos del poder nacional, para mantener o restablecer un ambiente seguro y proporcionar servicios esenciales de gobierno, reconstrucción de infraestructura de emergencia y asistencia humanitaria (MFRE 3-0). En la CI se ejecutan tareas para identificar, detectar y contrarrestar los factores de inestabilidad. Así mismo, mediante la contribución a los asociados de la AU, por medio de la unión de esfuerzos de inteligencia (UNESI), se desarrolla la recolección de información, para contribuir a las tareas de estabilización desarrolladas por la Fuerza, en apoyo a una nación anfitriona (en el exterior) o a un gobierno regional o local (dentro del territorio nacional), un gobierno transitorio o una autoridad militar de transición cuando no exista un gobierno legítimo (ver MFRE 3-0).

1.4.2.4. Tareas de apoyo de la defensa a la autoridad civil (ADAC)

[1-61] Las *tareas de apoyo de la defensa a la autoridad civil* son el soporte proporcionado por las Fuerzas Militares de Colombia y todas las instituciones que integran el sector defensa, en respuesta a solicitudes de asistencia de las autoridades civiles nacionales para emergencias domésticas de cualquier índole, apoyo a la imposición de la ley y otras actividades con entidades calificadas para situaciones especiales (MFE 3-28).

El apoyo a esta tarea estará determinado por la autorización del gobierno colombiano y, en dado caso, la CI podrá apoyar mediante las actividades dispuestas dentro de sus funciones, que puedan contribuir a afianzar la consolidación de uno o varios de los propósitos trazados por las tareas de ADAC.

ADAC

Apoyo de la defensa a la autoridad civil

1.4.3. La contrainteligencia en las funciones de conducción de la guerra

[1-62] Las *funciones de conducción de la guerra* son el conjunto de tareas y sistemas (personas, organizaciones, información y procesos) unidos por un propósito común, que los comandantes utilizan para cumplir misiones y objetivos de entrenamiento (MFE 3-0).

1.4.3.1. Función de conducción de la guerra Mando tipo misión

[1-63] Permite al comandante la integración, sincronización y articulación de los elementos del poder de combate, mediante la entrega de productos de CI que generen conocimiento sobre aspectos críticos de la operación acerca de las propias tropas que, de ser conocidos por el enemigo, llevarían al fracaso o limitarían el éxito de la operación. La CI suministra análisis estratégicos, operacionales y tácticos de interés, que brindan información oportuna para el proceso militar para la toma de decisiones (PMTD).

CI

Contrainteligencia

[1-64] La CI provee al comandante o a los tomadores de decisiones un amplio entendimiento acerca de los incidentes de CI y de las actividades de recolección de información de la inteligencia enemiga, las cuales se configuran como una amenaza para las operaciones, los medios dispuestos para la defensa nacional o el ejercicio del mando tipo misión; todo lo anterior repercute negativamente en la seguridad nacional.

1.4.3.2. Función de conducción de la guerra Movimiento y maniobra

CI | Contrainteligencia

[1-65] De ser necesario, se disponen agentes de CI para ser empleados dentro de las tareas de esta FCG, actuando de manera encubierta en un área determinada, que les permita recolectar y, posteriormente, aportar información relevante para obtener una relativa ventaja sobre el enemigo y facilitar el fortalecimiento de la sincronización de información de CI.

FCG | Función de conducción de la guerra

1.4.3.3. Función de conducción de la guerra Inteligencia

[1-66] La CI se configura como una de las diez disciplinas de la FCG Inteligencia, destinada a facilitar la comprensión de las actividades de las redes de inteligencia del enemigo y proporcionar a los comandantes en todos los escalones cursos de acción y medidas de seguridad que permitan proteger los activos críticos del Ejército. La CI apoya la inteligencia de todas las fuentes y se basa en otras disciplinas de la FCG Inteligencia para recolectar, analizar o procesar la información de CI.

1.4.3.4. Función de conducción de la guerra Fuegos

[1-67] La constrainteligencia apoya mediante el suministro y/o corroboración de ubicaciones (lugares) donde la amenaza esté desarrollando sus actividades y sean factibles las acciones de fuegos, con el propósito de crear efectos letales o no letales, según corresponda. Esta actividad se articula, a su vez, con el proceso de selección y priorización de blancos (PSPB), al proporcionar la identificación de los objetivos de interés para la Fuerza, sobre los cuales se requiere entregar apoyo de fuegos, según la necesidad. Además, apoya en la elaboración de la lista de recursos críticos (LRC) y lista de recursos defendidos (LRD), en ayuda al planeamiento de la defensa antiaérea.

1.4.3.5. Función de conducción de la guerra Sostenimiento

[1-68] La contrainteligencia se encargará de brindar información, que permita identificar o detectar los riesgos o vulnerabilidades presentes en el desarrollo de las actividades de sostenimiento, propendiendo por la protección de los activos críticos del Ejército y todo lo relacionado con los tres elementos principales de esta FCG: logística, servicios de personal y apoyo de servicios de salud, en donde se puedan presentar actos de subversión, sabotaje y/o espionaje.

FCG | Función de conducción de la guerra

1.4.3.6. Función de conducción de la guerra Protección

[1-69] Dentro del rol de la inteligencia y CI, se describe la tarea de apoyar la protección, la cual se desarrolla mediante la FCG Inteligencia y cuya función consiste en generar condiciones de seguridad destinadas a la preservación de la integridad, credibilidad y confiabilidad de los elementos que comprenden la Fuerza (información, personas, material, instalaciones, entre otros) (MFRE 2-0). De igual forma, se ejecutan diferentes tareas propias de la FCG Protección, como la implementación de procedimientos de seguridad militar, la cual se vale de las técnicas y procedimientos específicos para cada función y cuya finalidad es proteger y resguardar los activos críticos del Ejército; esto se desarrolla empleando el proceso de inteligencia y el proceso de gestión del riesgo.

CI | Contrainteligencia



ADN BICENTENARIO*

HISTORIA Y EVOLUCIÓN DE LA CONTRAINTTELIGENCIA EN EL EJÉRCITO NACIONAL

La contrainteligencia (CI) militar en Colombia tuvo su origen en 1964, con la fundación del Batallón de Inteligencia y Contrainteligencia (BINCI), el cual funcionó como un organismo homogéneo. Siendo esta una unidad pionera en implementar la CI en el ámbito militar en Colombia, se constituyó en un referente para la Fuerza Aérea y la Armada Nacional, que más adelante fundarían unidades especializadas de CI basadas en la experiencia del Ejército.

Fue hasta 1995 cuando se fundó la primera unidad de CI independiente de la inteligencia, y a la cual le fue asignado el nombre de Batallón de Contrainteligencia (BACI) y funcionó hasta finales de la misma década, cuando se crearon las centrales de cada una de las especialidades, entre las cuales se activó la Central de Contrainteligencia Militar (CECIM) y sus regionales, como unidades subordinadas.

Posteriormente, en 2014 la CECIM inició un proceso de transformación, que conllevó la activación de la Jefatura de Contrainteligencia (JECIM), el Comando de Contrainteligencia Militar, 2 unidades operativas menores y 28 unidades tácticas, que basaron su organización en la doctrina desarrollada en el Manual de Contrainteligencia Estratégica (MACIE).

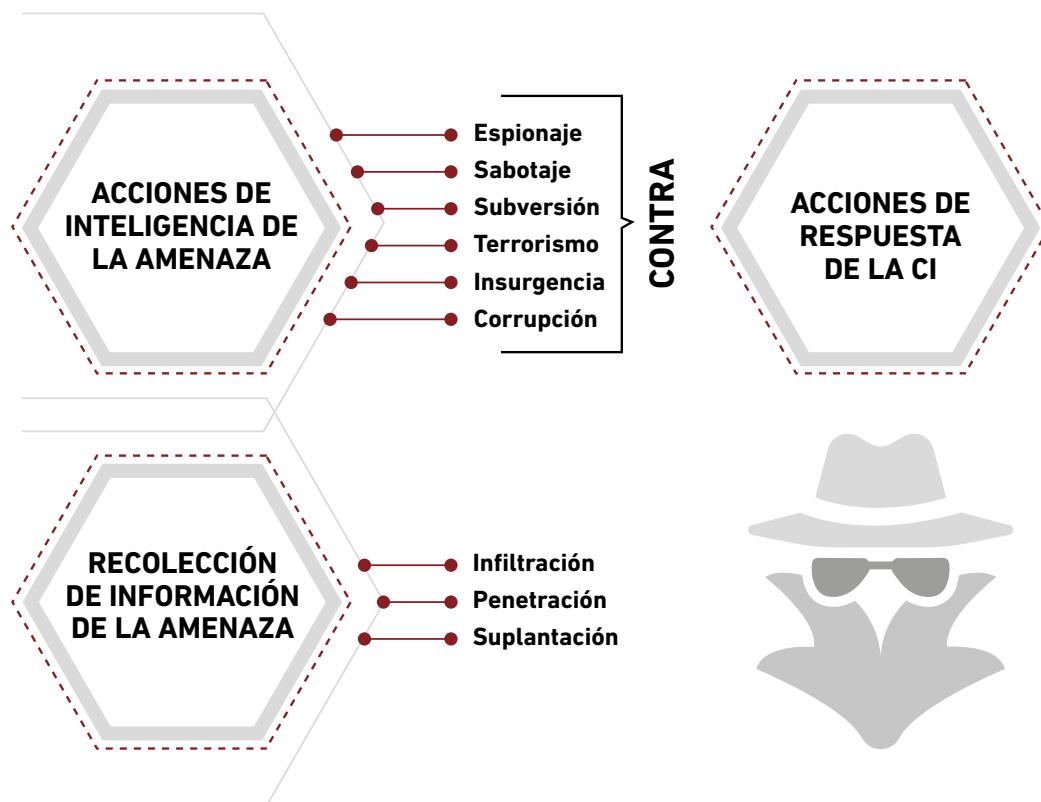
***Nota:** Este ícono acompaña los recuadros que contienen información histórica y doctrinal, que, a pesar de estar contenida en publicaciones que perdieron vigencia, se mantiene en el ADN del Ejército ayer, hoy y siempre. La doctrina Damasco construye sobre lo construido mientras reconoce y resalta con orgullo la experiencia de nuestros héroes.

CAPÍTULO 2

ACCIONES DE LA INTELIGENCIA DE LA AMENAZA Y ACCIONES DE RESPUESTA DE LA CONTRAINTELIGENCIA

"El origen de la inteligencia de los hombres reside en sus manos".

Anaxágoras



CI

Conrainteligencia

[2-1] Este capítulo aborda las acciones de inteligencia que suelen ser desarrolladas por la amenaza, las cuales se constituyen en objetivos para la ejecución de averiguaciones u operaciones de CI, mediante las acciones de respuesta pertinentes que se requieran en cada caso para la protección y seguridad de la Fuerza. Así mismo, plantea las técnicas empleadas por un adversario o una amenaza para recolectar información de su interés, las cuales pueden ser de uso común por parte de la comunidad de Inteligencia.

2.1. OBJETIVOS DE LA CONTRAINTELIGENCIA

[2-2] La amenaza ejecuta un indeterminado número de actividades para recolectar información de inteligencia o información de interés para el cumplimiento de sus planes, intenciones u órdenes provenientes de cualquier tipo de organización (servicios de inteligencia de otros Estados, servicios de seguridad, organizaciones de crimen transnacional, grupos criminales, grupos insurgentes y terroristas, entre otros), valiéndose de técnicas de infiltración, penetración o suplantación y empleando, según la necesidad, medios humanos o técnicos dispuestos para sus fines o intereses.

[2-3] Sin embargo, estas actividades se pueden resumir en un marco general y de fácil entendimiento, sin decir que estas son las únicas acciones que ejecuta la amenaza para cumplir sus objetivos, ya que de este marco general se desprenden una gran cantidad de indicadores, indicios o incidentes que revelan la acción de la amenaza y que variarán dependiendo del nivel estratégico, operacional o táctico en el cual se presenten.

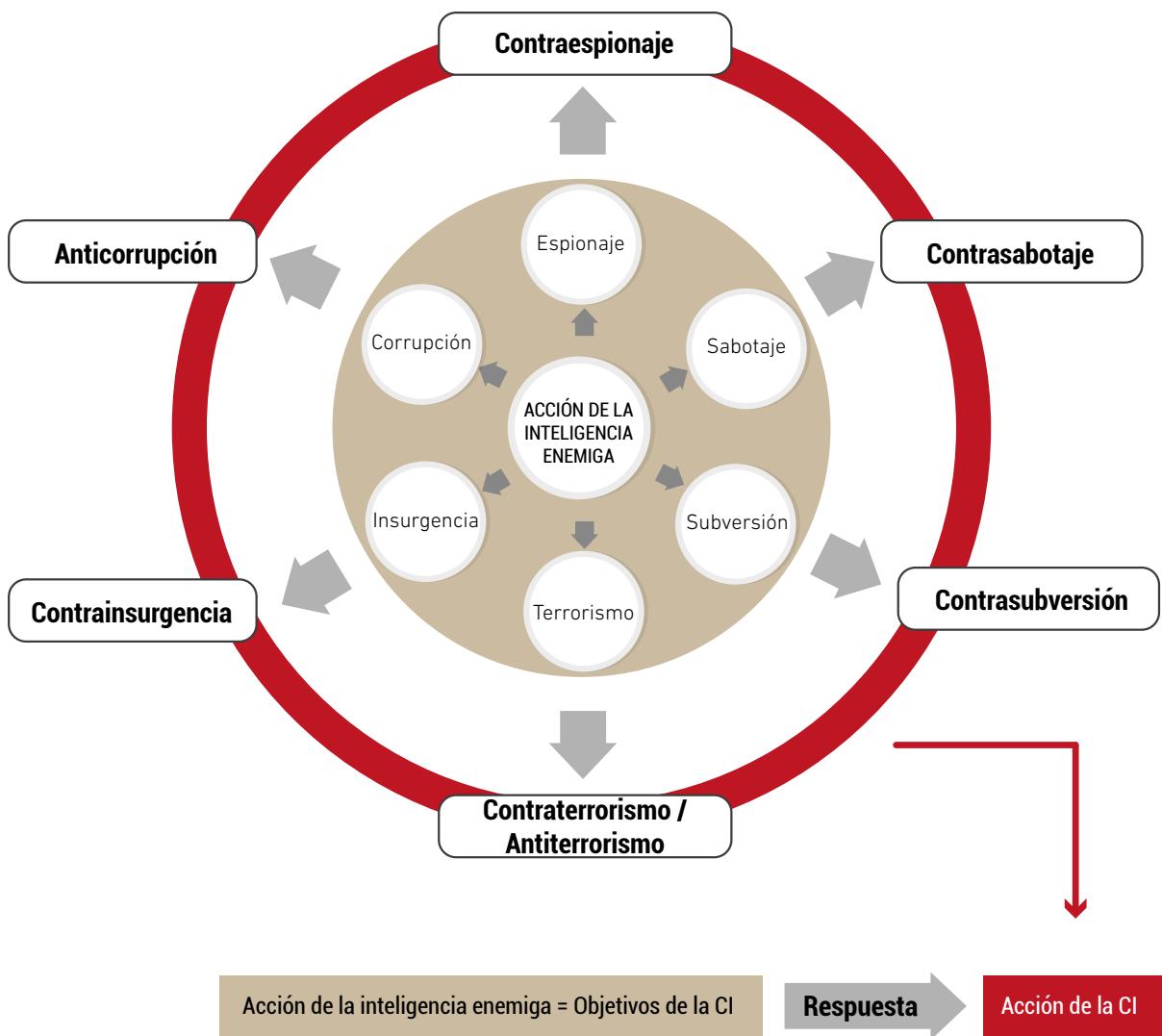
FISS
Inteligencia extranjera y servicios de seguridad

OT
Organizaciones terroristas

[2-4] Las principales acciones de inteligencia de la amenaza se constituyen en los objetivos de la contrainteligencia, los cuales producen la aplicación de acciones de respuesta de la CI definidas como la ejecución de actividades de CI conducidas para derrotar la recolección de información de FISS, OT, agentes locales y otras amenazas que tengan como finalidad realizar espionaje, subversión, sabotaje, terrorismo, insurrección o actividades de corrupción.

[2-5] Estas acciones de la CI se enfocan en realizar técnicas y procedimientos destinados a identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar cualquiera de las acciones enemigas a fin de proteger los **activos críticos del Ejército** definidos como el **conjunto de recursos que representan o generan un valor, compuesto por instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnologías de la información cuya inhabilitación o destrucción tendría un impacto negativo para el Ejército**.

CI | Contrainteligencia



| Figura 2-1 | Acciones de inteligencia de la amenaza y acciones de respuesta de la CI

2.1.1. Espionaje

[2-6] Es la actividad encaminada a obtener información clasificada o información de interés para quien la conserva o la busca.

[2-7] La inteligencia enemiga puede utilizar una o múltiples fuentes de inteligencia para obtener información, mediante el uso de medios físicos o virtuales, como señales y fuentes humanas y elementos de espionaje, como satélites, radares, sensores, cámaras o cualquier medio con el que puedan recolectar información.

[2-8] La infiltración y la penetración son las técnicas más comúnmente utilizadas por la amenaza; sin embargo, esta actividad también puede ser desarrollada por una persona sin entrenamiento, pero que encuentra la oportunidad para hurtar información en beneficio propio o de terceros, usualmente relacionada con:

- Planes de guerra, operacionales, estatales u otros planes de interés.
- Ubicación y funcionamiento de unidades militares o infraestructura crítica.
- Elementos usados para la defensa nacional.
- Redes de inteligencia propias (personal, material, equipos, instalaciones, etc.).
- Métodos de recolección de información propios.
- Información de operaciones, inteligencia, personal, sosténimiento, estabilidad o de cualquier otra índole o aspecto del Ejército que sirva al enemigo para la materialización de sus intenciones.

| Tabla 2-1 | Espionaje y contraespionaje

Espionaje	Actividad encaminada a obtener información reservada o clasificada para quien la conserva o la busca.
Contraespionaje	Acción que tiene como finalidad negar al adversario el acceso a la información reservada o clasificada del Ejército o de los asociados de la acción unificada.
Finalidad de la CI	Contrarrestar la capacidad del adversario de atacar eficazmente los objetivos o planes propios a todo nivel, relacionados con información de interés obtenida del Ejército de forma irregular, la cual puede ser empleada para afectar el personal, las operaciones, el material o cualquier otro activo estratégico de la Fuerza.
Acciones de la amenaza	<ul style="list-style-type: none"> • Divulgar la identidad de agentes, agencias o métodos utilizados por agentes de inteligencia o CI a personal no autorizado. • Copiar, tomar u obtener información de las unidades militares o de las operaciones por medio de solicitudes de información clasificada sin la debida autorización del superior jerárquico o mediante cualquier otro tipo de actividad irregular. • Comunicar, entregar, transmitir, recolectar, registrar o publicar información con respecto al movimiento, números, descripción, condición o disposición de las propias tropas, equipo o material. • Fotografiar, filmar, dibujar, georreferenciar o crear una representación gráfica de instalaciones y equipos militares, para su publicación, venta o empleo en actividades de inteligencia o CI que afecten al Ejército. • Recibir, obtener o aceptar cualquier tipo de beneficio de personas, organizaciones o fuentes que tenga relación con intenciones de recibir información sobre las unidades militares, operaciones militares, personal de la Fuerza o cualquier otro activo crítico del Ejército. • Remover, reclasificar, reorganizar, modificar o alterar material clasificado de los archivos del Ejército o de los asociados de la acción unificada. • Efectuar actividades de suplantación del personal militar o civil que trabaja en el Ejército, con cualquier fin. • Acceder a los sistemas de información sin autorización, así como la intrusión de elementos electrónicos o dispositivos de escucha en instalaciones militares. • Omitir o no reportar la pérdida de información reservada o clasificada del Ejército, con la finalidad de permitir la acción de la inteligencia enemiga.

TIPOS DE SABOTAJE

Para generar daños al ecosistema

Económico

A corredores de movilidad

A los servicios públicos

Paro armado

2.1.2. Sabotaje

[2-9] Es el daño o deterioro que se hace en instalaciones, productos, etc., o procedimiento de lucha contra la autoridad (contra los patronos, el Estado o las fuerzas de ocupación en conflictos sociales o políticos) (MCE 3-24.0).

[2-10] Las acciones de sabotaje necesitan personal que realice estudios previos y adquiera información de inteligencia para poder ejecutarlos. Los tipos de sabotaje son:

- Sabotaje para generar daños al ecosistema.
- Sabotaje económico.
- Sabotaje a corredores de movilidad.
- Sabotaje a los servicios públicos.
- Paro armado.

[2-11] Así mismo, la inteligencia de la amenaza utiliza los siguientes métodos para materializar los actos de sabotaje:

- Incendiario: uso de fuego.
- Explosivo: uso de artefactos explosivos.
- Mecánico o hidráulico: sustracción o adición de elementos para afectar el funcionamiento de una máquina.
- Electrónico: uso de recursos electrónicos.
- Cibernético: empleo de *malware* y ejecución de código remoto.

[2-12] También pueden considerarse como actos de sabotaje aquellos en los cuales se realicen, retrasen u omitan acciones propias de las funciones de un cargo, que lleven a un daño o deterioro de un equipo, de material técnico, de maquinaria o de una instalación del Ejército.

MÉTODOS PARA MATERIALIZAR ACTOS DE SABOTAJE

Incendiario

Explosivo

Mecánico o hidráulico

Electrónico

Cibernético

| Tabla 2-2 | Sabotaje y contrasabotaje

Sabotaje	Daño o deterioro que se hace en instalaciones, productos, etc., o procedimiento de lucha contra la autoridad (contra los patronos, el Estado o las fuerzas de ocupación en conflictos sociales o políticos) (MCE 3-24.0).
Contrasabotaje	Acción de contrarrestar el daño, deterioro o destrucción total o parcial del poder de combate, los activos críticos del Ejército o la infraestructura crítica de la nación.
Finalidad de la CI	Identificar e interrumpir los planes, intenciones, programas o cualquier actividad que pueda convertirse en una amenaza de sabotaje. De igual forma permite aportar información acerca de incidentes relacionados con acciones de sabotaje, que puedan servir para la construcción de planes o programas de seguridad.
Acciones de la amenaza	<ul style="list-style-type: none"> • Dañar, destruir o afectar cualquier material de guerra con la intención de perjudicar u obstruir la capacidad militar de una unidad. • Producir cualquier material de guerra o influir para que se elabore de manera defectuosa, con la intención de perjudicar, interferir u obstruir las operaciones militares. • Dañar o destruir propiedades militares, instalaciones, elementos técnicos, de comunicaciones o cualquier otro que sea vital para el cumplimiento de la misión.

2.1.3. Subversión

[2-13] Es el conjunto de acciones diseñadas para debilitar la fortaleza o la moral militar, económica, psicológica o política de una autoridad gobernante (MCE 3-24.0).

[2-14] En muchas ocasiones, las actividades subversivas son el primer paso para convencer a una persona o a un grupo de personas de alzarse violentamente contra una o varias instituciones legalmente constituidas. Es decir, algunos grupos de la amenaza utilizan la subversión para apoyar sus conceptos políticos, ideológicos o sociales, de los cuales se valen para realizar el reclutamiento de personal para diferentes actividades criminales o indebidas contra la institución.

| Tabla 2-3 | Subversión y contrasubversión

Subversión	Conjunto de acciones diseñadas para debilitar la fortaleza o la moral militar, económica, psicológica o política de una autoridad gobernante (MCE 3-24.0).
Contrasubversión	Acción para negar el desarrollo de actividades del enemigo, que busquen debilitar la competencia, el carácter, el compromiso, la cultura, la ética y la moral del Ejército o de los asociados de la acción unificada. También se incluyen aquellas actividades destinadas a la desinformación o la implantación de ideologías adversas al Ejército.
Finalidad de la CI	La CI ejecuta actividades para disminuir, anular o bloquear las acciones de la amenaza que pretendan realizar o influenciar a otro para que realice actos de subversión. Esto lo hace la CI identificando individuos o grupos de personas que, mediante cualquier método, busquen influir en el comportamiento de un grupo de personas para que actúen de forma violenta contra el Estado social de derecho legalmente constituido, sus instituciones o sus intereses.
Acciones de la amenaza	<ul style="list-style-type: none"> • Influir en las propias tropas con el fin de causar insubordinación, deslealtad, motín o rechazo del deber por parte de cualquier miembro del Ejército o con la intención de interferir, perjudicar o influenciar la lealtad, la moral o la disciplina del personal militar. • Hacer o transmitir deliberadamente informes o declaraciones falsas con la intención de interferir en las operaciones militares, afectar la moral de las tropas o cualquier otro fin que altere la normalidad de las actividades de la institución. • Fomentar el sindicato y la indisciplina táctica dentro de la Fuerza, alterar el orden y la disciplina o negarse a obedecer las órdenes, con la intención de derrocar la autoridad militar legal. • Conocer, tener indicios o presenciar una intención o materialización de motín o sedición y omitir la realización de las acciones pertinentes para prevenir, informar y/o controlar la conducta. • Distribuir y difundir información falsa para lograr que una persona o una organización cambie de opinión. • Difundir ideologías políticas o religiosas extremistas que logren cambiar el actuar o el pensar de una persona. • Ofrecer cualquier tipo de beneficio para realizar actividades ilícitas. • Manipulación de comunidades para incitarlos a la protesta social violenta o asonada en contra de la Fuerza o del gobierno.

[2-15] La subversión se puede manifestar bajo las siguientes actividades: huelga, disturbio, asonada y/o motín (MCE 3-24.0).

[2-16] La subversión es una de las principales actividades utilizadas por la amenaza para recolectar información o vulnerar los sistemas de seguridad del Ejército o de los asociados de la AU. Se han logrado establecer los siguientes indicadores para determinar que una persona está siendo

AU | Acción unificada

influenciada por grupos subversivos o que está tratando de subvertir a otros:

- Fuga de información.
- Difusión de información falsa, subversiva o propaganda por cualquier medio a otras personas de la organización.
- Actividades de corrupción.
- Tráfico o pérdida de material de guerra, intendencia o cualquier elemento de uso privativo de las Fuerzas Militares.
- Incremento injustificado de bienes.
- Cambios negativos en su comportamiento, que se encuentren en contravía con los principios y valores del Ejército.

2.1.4. Terrorismo

[2-17] Es el uso ilegal de la violencia o de la amenaza de violencia, a menudo motivado por creencias religiosas, políticas o ideológicas, para difundir terror e imponer a los gobiernos o las sociedades la búsqueda de objetivos generalmente políticos (MCE 3-24.0).

[2-18] Existen cuatro tipos de terrorismo dependiendo de los actores que lo ejecutan: político, de Estado, de guerra y narcoterrorismo (ver el MCE 3-24.0 para ampliar esta información).

[2-19] Los grupos terroristas usan métodos y técnicas similares a los que emplean los servicios de inteligencia o las agencias de seguridad para recolectar información de interés, así:

- Estudio del ambiente donde desarrollan actividades de recolección.
- Reclutamiento de personas que simpaticen con la causa del grupo o con la célula terrorista que se encuentre en el área.

- Uso de identificaciones falsas, creación de fachadas e historias del personaje con el fin de cometer acciones en contra del Ejército.
- Uso de células o grupos pequeños para recolectar información (las células terroristas encargadas de recolectar información también pueden ejecutar los actos terroristas).
- Manipulación y aprovechamiento de grupos de especial protección para lograr recolectar información o ejecutar actos terroristas.

[2-20] El terrorismo es llevado cabo con los siguientes objetivos (sin ser los únicos):

- Alcanzar propósitos políticos, económicos, ideológicos o religiosos.
- Obligar a alguna organización a realizar o a omitir un determinado acto.
- Propagar el miedo y, con ello, limitar el derecho a la oposición.
- Obligar a un enemigo a rendirse.
- Detener el actuar de los servicios de inteligencia, de las Fuerzas Militares o de los entes judiciales para poder realizar actividades delincuenciales sin acción de respuesta de fuerzas legítimas.
- Encubrir actividades de recolección de información.

ACTIVOS CRÍTICOS DEL EJÉRCITO

Conjunto de recursos que representan o generan un valor, compuesto por instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnologías de la información cuya inhabilitación o destrucción tendría un impacto negativo para el Ejército (MCE 2-22.1).

INFILTRACIÓN

Técnica que emplea la amenaza para introducir una persona dentro de una organización con el fin de obtener información (MCE 2-22.1).

PENETRACIÓN

Técnica que emplea la amenaza para lograr que una persona ejecute acciones adversas a la organización a la que pertenece (MCE 2-22.1).

SUPLANTACIÓN

Técnica utilizada para sustituir de manera ilegal un elemento, sistema o persona para obtener algún beneficio (MCE 2-22.1).

| Tabla 2-4 | Terrorismo y contraterrorismo

Terrorismo	Uso ilegal de la violencia o de la amenaza de violencia, a menudo motivado por creencias religiosas, políticas o ideológicas, para difundir terror e imponer a los gobiernos o las sociedades la búsqueda de objetivos generalmente políticos (MCE 3-24.0).
Contraterrorismo / Antiterrorismo	<p>Contraterrorismo: Acciones militares ofensivas para prevenir, detener y responder a las acciones terroristas, atacando en forma directa su infraestructura y redes de apoyo, y de manera indirecta para influenciar ambientes regionales y globales para restringir su empleo por parte de redes terroristas (MFRE 3-05).</p> <p>Antiterrorismo: Medidas defensivas utilizadas para reducir la vulnerabilidad de las personas y los bienes en caso de actos terroristas; su objetivo es suprimir el terrorismo mediante una acción rápida por parte de las fuerzas militares y de las autoridades civiles y locales (MCE 3-24.0).</p>
Finalidad de la CI	Interrumpir, contrarrestar o neutralizar las acciones de terrorismo llevadas a cabo por cualquier tipo de amenaza con el fin de proteger la población civil y los activos críticos del Ejército.
Acciones de la amenaza	<ul style="list-style-type: none"> • Asesinar o atentar contra la integridad física de militares colombianos de cualquier forma; por ejemplo, mediante artefactos explosivos improvisados (AEI), envenenamiento, homicidio intencional, uso de terceras personas, entre otras. • Producir o elaborar artefactos explosivos no convencionales para ser utilizados en acciones que alteren el orden público. • Desarrollar acciones violentas que vayan en contra de la seguridad pública. • Proporcionar recursos económicos o de otra índole a grupos terroristas o grupos armados organizados que tengan la intención de atentar contra las propias tropas. • Participar en conspiraciones para atacar una patrulla o una instalación militar o cualquier activo del Ejército, mediante cualquier método de ataque. • Secuestrar personal militar. • Participar en tortura de personal militar, ya sea que se encuentre como prisionero de guerra o en cumplimiento de actividades de inteligencia y contrainteligencia.

2.1.5. Insurgencia

[2-21] Son las acciones de un grupo o movimiento organizado, normalmente ideológicamente motivado, que busca afectar o prevenir un cambio político o derrocar una autoridad gubernamental dentro de un país o región, enfocado en persuadir o coaccionar a la población mediante el uso de la violencia y la subversión (MCE 3-24.0).

[2-22] Estos grupos se escudan en causas revolucionarias, ideológicas, sociales o religiosas para tratar de tomar control de territorios y/o instituciones; normalmente son de carácter secreto o clandestino, razón por la cual utilizan medios y métodos similares a los servicios de inteligencia, para proteger su identidad y sus actividades.

[2-23] Los grupos insurgentes son el resultado de un proceso de organización que se va fortaleciendo conforme a la trayectoria de sus acciones, dado que podrían estar empleando para la consecución de sus objetivos la guerra popular prolongada que tiene como objetivo resistir en el tiempo y espacio para desgastar al enemigo, razón por la cual estos grupos tienen tiempo suficiente para organizarse y ganar más adeptos. Usualmente estos grupos funcionan como una organización político-militar y tienen unos subgrupos o células divididas así:

- Organización militar.
- Organización política.
- Células de inteligencia.
- Grupos de apoyo logístico.
- Células de contrainteligencia.
- Células de grupos armados (no uniformados).
- Organización de movimiento popular o de masas.
- Grupos de adoctrinamiento ideológico, político o religioso.
- Grupo de reclutadores.
- Grupo de gestión de finanzas.

[2-24] Algunos de los grupos cuentan con uno, varios o todos los elementos anteriormente nombrados, dependiendo de su evolución, de la causa, del apoyo externo o del número de integrantes. Estos elementos también harán que dichos grupos empleen la combinación de todas las formas de lucha para conseguir sus objetivos.

| Tabla 2-5 | Insurgencia y contrainsurgencia

Insurgencia	Acciones de un grupo o movimiento organizado, normalmente ideológicamente motivado, que busca afectar o prevenir un cambio político o derrocar una autoridad gubernamental dentro de un país o región, enfocado en persuadir o coaccionar a la población mediante el uso de la violencia y la subversión (MCE 3-24.0).
Contrainsurgencia	Son esfuerzos civiles y militares realizados para derrotar una insurgencia y hacer frente a posibles daños importantes (MFRE 3-05) En la contrainsurgencia se realizan acciones militares conducidas para enfrentar la resistencia armada de un grupo insurgente, para reestablecer la autoridad legítima del Estado con apoyo político, económico y social. Se requiere para ello fortalecer la comprensión situacional basada en experiencia regional, habilidades especiales de combate, capacidad de interactuar con la nación anfitriona y su población civil.
Finalidad de la CI	Impedir o interrumpir el direccionamiento de grupos insurgentes y el accionar de sus redes de apoyo mediante el desarrollo actividades de desinformación y operaciones de deserción. De igual manera efectúa los diagnósticos de debilidades y vulnerabilidades existentes en el personal de la Fuerza, que puedan permitir o facilitar acciones insurgentes con el empleo de elementos propios del Ejército.
Acciones de la amenaza	<ul style="list-style-type: none"> • Uso de armas no convencionales. • Alteración del orden público. • Empleo de manifestaciones violentas con fines insurgentes. • Actividades de espionaje, sabotaje o subversión. • Guerra de guerrillas. • Desinformación a las instituciones legalmente constituidas. • Invitación al odio a través de la ideología de "lucha de clases". • Adocinaramiento insurgente en colegios y/o universidades. • Realizar actividades de inteligencia delictiva. • Reclutamiento de servidores públicos para atacar las instituciones desde su interior. • Uso de menores para cometer actividades ilícitas. • Actuación a nombre de otras organizaciones.

2.1.6. Corrupción

[2-25] Es la práctica consistente en la utilización indebida de cargos, funciones y/o medios en provecho económico o de otra índole para un grupo determinado o para el suyo propio, la cual podrá manifestarse en el intercambio de favores contrarios a la ética, entre quien desempeña una labor y quienes adelanten de forma lícita o ilícita una actividad que se encuentre en contravía de los propósitos del Ejército.

| Tabla 2-6 | Corrupción y anticorrupción

Corrupción	Práctica consistente en la utilización indebida de las funciones y medios en provecho económico o de otra índole para un grupo determinado o para el suyo propio, la cual podrá manifestarse en el intercambio de favores contrarios a la ética, entre quien desempeña un cargo o labor y quienes adelantan de forma lícita o ilícita una actividad que se encuentre en contravía de los propósitos del Ejército.
Anticorrupción	Conjunto de actividades diseñadas para combatir la omisión, extralimitación o acción irregular de las funciones de miembros de la Fuerza que busquen recibir algún beneficio que no corresponda a la ética y la moral.
Finalidad de la CI	Identificar indicios o incidentes de corrupción, para recolectar información que lleve a neutralizar actividades de corrupción administrativa que afecten las operaciones militares o la imagen institucional.
Acciones de la amenaza	<ul style="list-style-type: none"> • Incumplir las normas legales o institucionales en el proceso de selección e incorporación, así como permitir que a las escuelas de formación o a la institución ingrese o se vincule (en cualquiera de las formas) personal que no cumpla con el perfil de seguridad necesario para laborar en el Ejército. • Divulgar o filtrar información reservada o clasificada, documentos, expedientes, planes operacionales, resultados de los exámenes de credibilidad y confiabilidad, entre otros, que pueda afectar la integridad del personal o el desarrollo de actividades sensibles de la Fuerza. • Cometer fraudes identificados (suplantación, adulteración, manipulación, modificación, adición o eliminación) en documentos que sirven de soporte para trámites administrativos y presupuestales, así como en los sistemas de información en la administración del talento humano. • Elaborar y enviar documentación falsa para la solicitud de asignación de recursos, partidas, primas u otros aspectos de manera fraudulenta y con fines diferentes a los establecidos dentro de la ley. • Cometer fraudes identificados (adulteración, manipulación, modificación, adición o eliminación) en los sistemas de información empleados por el Ejército en cualquiera de las áreas de uso (Inteligencia, Armamento, Intendencia, Sanidad, entre otras). • Cometer corrupción administrativa asociada a la asignación, uso, empleo o disposición de la partida de gastos reservados. • Recibir cualquier beneficio personal con ocasión de la celebración de un contrato, así como el pago de recursos de acreedores varios a terceros diferentes al beneficiario final. • Constreñir, inducir, dar, prometer o recibir dinero o cualquier utilidad indebida por la administración, asignación o desviación injustificada de elementos y/o materiales del Ejército (armamento, intendencia, comunicaciones, material aeronáutico, repuestos de cualquier tipo, entre otros). • Uso indebido de bienes fiscales en custodia del Ejército Nacional.

CI

Contrainteligencia

[2-26] A diferencia de las anteriores, esta no es una acción de inteligencia de la amenaza. Sin embargo, la CI asume esta acción como uno de sus objetivos, ya que puede afectar a todo el personal (oficiales, suboficiales, soldados, auxiliares, contratistas y/o personal civil) que se encuentre vinculado al Ejército, debido a que pueden realizar actividades ilícitas valiéndose de su ubicación, acceso, manejo, influencia o cualquier otra relación existente con medios o recursos de la institución, lo cual perjudica la integridad y transparencia en los procesos.

[2-27] La contrainteligencia militar apoya la lucha contra la corrupción; sin embargo, esta lucha es responsabilidad inherente a todos los funcionarios quienes tienen la obligación de denunciar todo acto irregular conocido e implementar todas las medidas necesarias para evitar las manifestaciones de estas acciones dentro del Ejército.

2.2. RECOLECCIÓN DE INFORMACIÓN DE LA AMENAZA

[2-28] Las redes de inteligencia de la amenaza realizan diferentes actividades para recolectar información de interés del Ejército o de los asociados de la acción unificada (AU), así como de seguridad pública, seguridad nacional o que afecte la defensa nacional; para ello pueden emplear medios humanos o técnicos. El desarrollo de una u otra técnica dependerá del análisis que la amenaza efectúe sobre el ambiente operacional y de la oportunidad prevista en debilidades y vulnerabilidades de la Fuerza, que faciliten o permitan recolectar información.

[2-29] Las técnicas que a continuación se relacionan pueden ser desarrolladas por la amenaza a través de medios humanos; sin embargo, existirán otras que podrán emplear medios digitales, como el ciberespacio, el espectro electromagnético (EEM) o el espectro radioeléctrico, entre otros.

2.2.1. Infiltración

[2-30] La **infiltración** se define en inteligencia como la **técnica que emplea la amenaza para introducir una persona dentro de una organización con el fin de obtener información**. La información recolectada por un infiltrado es considerada de alta credibilidad, ya que el elemento o la persona tendrá acceso privilegiado a información que mediante otras técnicas es difícil de recolectar. Usualmente, el infiltrado deberá tener altos conocimientos en técnicas de recolección de información, así como conocimiento minucioso de la organización, los procesos y el funcionamiento de esta.

[2-31] Estas son algunas de las conductas, comportamientos o actuaciones que puede presentar un infiltrado en el Ejército, los cuales representan indicadores de su actividad para la CI:

- Su lugar de origen tiene influencia subversiva o es dominado por tendencias delictivas.
- Busca llegar a cargos u oficinas donde se maneje un alto nivel de seguridad o se allegue información privilegiada.
- Evita discusiones moralistas, ideológicas o alguna en la que se traten temas que tengan que ver con su causa.
- Busca áreas seguras para recibir o realizar llamadas.
- Trabaja en horas diferentes a las estipuladas por el horario de régimen interno, dado que cuando el flujo de personal disminuye, esto le facilita el acceso a la información, material, equipos o cualquier activo de interés para la amenaza.
- No se tiene clara su procedencia ni sus relaciones fuera del ámbito laboral, por lo cual evita continuamente el hablar de su pasado, sus relaciones familiares, sus tendencias ideológicas o cualquier tema de carácter personal que pueda ponerlo al descubierto.

CI

Contrainteligencia

- Evita situaciones sociales que puedan exponerlo a circunstancias incómodas donde tenga que revelar información personal.
- Busca crear amistades cercanas, muchas veces sentimentales con personas que manejen información de interés.
- Se relaciona no abiertamente con funcionarios que sean dependientes del alcohol, que tengan problemas económicos, adicciones o que sean vulnerables de alguna forma, para tratar de reclutarlos.
- Se caracterizan por mantener un sobresaliente y constante nivel de trabajo; se presentan como líderes de conducta amable y complaciente tanto con sus superiores como con sus compañeros y subordinados, con el fin de ganar la confianza necesaria para efectuar sus actividades irregulares.

[2-32] A continuación se presentan algunas de las actividades que se deben adoptar para evitar la infiltración dentro del Ejército:

- Tener protocolos de ingreso con altos estándares de credibilidad y confiabilidad, en los cuales se incluya la presentación de pruebas técnicas psicofisiológicas de veracidad como requisito de ingreso y las cuales se mantengan durante el tiempo que dure la vinculación de la persona con la Fuerza.
- Mantener los servicios de base de datos de CI actualizados empleándolos para verificación de personal de aspirantes en los procesos de ingreso y vinculación.
- Establecer redes de CI dentro de la institución para monitorear actividades sospechosas de los funcionarios.
- Cumplir los protocolos de seguridad de la información.
- Compartimentar la información y, si es necesario, desinformar a ciertas secciones o grupos de personas.

- Ejecutar el procedimiento de contraespionaje del equipo rojo, para descubrir vulnerabilidades propias.

2.2.2. Penetración

[2-33] La **penetración** se define en inteligencia como la **técnica que emplea la amenaza para lograr que una persona ejecute acciones adversas a la organización a la que pertenece**. El penetrado normalmente tiene acceso a información privilegiada.

[2-34] Estas son algunas de las conductas, comportamientos o actuaciones que puede presentar un penetrado en el Ejército, los cuales representan para la CI indicadores de su actividad:

- Manipula, cambia o altera información que pueda afectar sus intereses.
- Busca áreas seguras para recibir o realizar llamadas.
- Cambia su nivel de vida súbitamente, paga deudas de forma intempestiva sin razón creíble.
- Ostenta un nivel de vida que de acuerdo con su salario e ingresos reconocidos no puede sustentar.
- Trata de establecer lazos de amistad o cercanía con personal de inteligencia o CI.
- Se caracteriza por intentar congraciarse o ganarse la favorabilidad de superiores, compañeros y subordinados mediante obsequios o conductas complacientes, adquiriendo de esta forma la confianza necesaria para facilitar la realización de actividades irregulares.

CI

Contrainteligencia

[2-35] Las redes de inteligencia de la amenaza estudian previamente a las personas que pueden ser reclutadas. y para ello, tienen en cuenta sus vulnerabilidades y las motivaciones de carácter económico, ideológico, social, político, familiar o laboral que necesitan satisfacer, para que estas

colaboren o trabajen con la organización. Es necesario tener en cuenta que para una persona un viaje puede ser una motivación; para otras, un incremento en su salario o un ascenso, pero también la adquisición de un medicamento, el reconocimiento social, la venganza o cualquier otra razón, debido a las adversidades y necesidades que enfrentan en su cotidianidad. Es objeto de análisis e identificación de cuáles de esas motivaciones pueden ser explotadas satisfactoriamente al representarle a la amenaza un acceso directo o indirecto a un activo estratégico o de interés del Ejército.

[2-36] A continuación, se presentan algunas de las actividades necesarias para evitar la penetración dentro del Ejército.

CI | Contrainteligencia

- Emplear y adelantar actividades de la disciplina de CI por medio de las redes internas de las unidades.
- Realizar entrevistas de CI a personal retenido o a fuentes que puedan tener información acerca de posibles penetrados.
- Realizar actividades permanentes de seguridad militar.
- Evaluar periódicamente a los funcionarios con pruebas técnicas psicofisiológicas de veracidad.
- Verificar los estudios de seguridad de personal y los estudios socioeconómicos de los funcionarios y emitir recomendaciones al comandante respecto al resultado de estos.
- Implementar contramedidas de vigilancia electrónica.
- Cumplir los protocolos de seguridad de la información.

2.2.3. Suplantación

[2-37] La ***suplantación*** se define como la **técnica utilizada para sustituir de manera ilegal un elemento, sistema o persona para obtener algún beneficio**. La suplantación también se puede presentar en el dominio del ciberespacio.

[2-38] Entre los objetivos de la suplantación se encuentran los siguientes (sin ser los únicos):

- Obtener información privilegiada.
- Identificar personas, organizaciones o locaciones
- Recolectar información de los procedimientos de seguridad.
- Reclutar fuentes de información.
- Ejecutar actos terroristas.
- Implantar elementos técnicos de escucha.
- Transportar mercancía ilegal o material de guerra.
- Obtener beneficios personales.

[2-39] En la actualidad, la forma más común de suplantación es a través de redes sociales o servicios de información, lo cual se denomina *phishing* y se pueden realizar ataques cibernéticos a través de servidores falsos, cuentas falsas u otros métodos para lograr acceder a la información contenida en los equipos de cómputo, en la nube o en cualquier sistema de almacenamiento.

[2-40] Estas son algunos de las recomendaciones para evitar la suplantación:

- Implementar procedimientos de seguridad militar.
- Incrementar las actividades de seguridad física.
- Realizar actividades de seguridad de información pertinentes para el cuidado y protección de este activo.
- Mantener bases de datos actualizadas y debidamente custodiadas.
- Implementar ficheros de identificación que tengan consignada información como la unidad, la dependencia y el cargo.

- Velar por la protección de datos de la institución y del personal.
- Crear conciencia acerca de la necesidad de autoprotección relacionada con el resguardo y manejo adecuado de datos personales y familiares.
- Desarrollar capacitaciones relacionadas con la suplantación, dirigidas especialmente al personal de oficiales, suboficiales y soldados responsables de los dispositivos de seguridad en cada una de las unidades militares.



AFFECTACIÓN A LAS REDES DE APOYO

La noche del 14 de abril de 2015, un grupo perteneciente a la estructura armada de la entonces denominada guerrilla de las FARC llevó a cabo una acción militar en contra de una patrulla del Ejército Nacional que se encontraba pernoctando en el polideportivo de la vereda La Esperanza, del municipio de Buenos Aires (Cauca). El hecho dejó como resultado 11 militares muertos y 17 heridos, lo que provocó una crisis en el proceso de paz que se adelantaba en la Habana, Cuba, entre el gobierno colombiano y la guerrilla de las FARC.

En consecuencia, la CI inicia una serie de actividades por medio de las cuales se logra establecer que gran parte de la munición, las granadas y las armas empleadas por esta guerrilla para ejecutar el ataque pertenecían al Ejército Nacional. La información obtenida hasta el momento dio paso a la identificación y la posterior captura de varias personas que hacían parte de las redes de inteligencia del frente de las FARC que operaba en esa zona del país, y quienes fueron las responsables de suministrar la información acerca del dispositivo, la composición, la Fuerza y las vulnerabilidades de la patrulla del Ejército que fue atacada.

Por último, la información obtenida inicialmente acerca del lote y la serie de la munición conllevo la identificación de militares activos que estarían suministrando el material de guerra al componente armado de la amenaza. El resultado de esta operación condujo a la captura de siete militares activos que desempeñaban el cargo de almacenistas de armamento en diferentes unidades militares en todo el país, y quienes acusaron, a su vez, a tres personas ajenas a la institución de ser las encargadas de transportar el material de guerra hasta las zonas campamentarias de los grupos insurgentes. Estos últimos también fueron capturados.

CAPÍTULO 3

OPERACIONES DE CONTRAINTELIGENCIA

"Hoy la prueba real de poder no es la capacidad de hacer la guerra, sino la capacidad de prevenirla".

Anne O'Hare McCormick



3.1. GENERALIDADES

[3-1] Las ***operaciones de contrainteligencia*** se definen como la **secuencia de acciones tácticas para la recolección de información sobre las acciones de inteligencia de la amenaza y los indicios de corrupción al interior de la Fuerza**. De acuerdo con las acciones de la amenaza (ver capítulo 2), los comandantes de la contrainteligencia (CI) deberán determinar qué técnicas o procedimientos requieren efectuar para cumplir con las actividades de identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar.

CI | Contrainteligencia

[3-2] Las acciones de respuesta de la CI, que se encuentran desarrolladas en el capítulo 2, se configuran como operaciones de CI siempre y cuando se ejecute una secuencia de acciones tácticas con un propósito común, si se entiende “acciones tácticas” como la ejecución simultánea de técnicas y procedimientos de CI.

[3-3] En este entendido, las clases de operaciones de CI serán de: contrasubversión, contrasabotaje, contraespionaje, contraterrorismo, contrainsurgencia y anticorrupción, siempre y cuando se cumplan los parámetros para su configuración y su desarrollo establecidos en el procedimiento operacional de CI.

OTU | Operaciones terrestres unificadas

[3-4] Las operaciones de CI se llevan a cabo dentro del concepto operacional del Ejército (operaciones terrestres unificadas [OTU]), donde dichas operaciones asumen una función indispensable al constituirse en el principal recurso del Ejército para planear y configurar las acciones de protección de las tropas, y permitir de esta manera el libre desarrollo de la maniobra en el dominio terrestre.

ADAC | Apoyo de la defensa a la autoridad civil

[3-5] El concepto de OTU se fundamenta en la sincronización de tareas ofensivas, defensivas, de estabilidad y ADAC para aplicar el poder terrestre como parte de la AU y derrotar el enemigo en tierra. En este entendido, las operaciones de CI cumplen un papel fundamental para el desarrollo de las diferentes tareas del Ejército, ya que ninguna de ellas puede ser ejecutada sin haber determinado previamente la capacidad

del adversario de conocer los planes operacionales de las propias tropas. Al ser este el rol de las operaciones de CI dentro del marco de la acción decisiva, dichas operaciones se consideran un elemento clave para el ejercicio del mando tipo misión, pues aportan información fundamental a la seguridad de las operaciones. La CI, valiéndose de sus competencias distintivas, sus funciones y sus servicios técnicos, brinda el soporte necesario de acuerdo con las necesidades existentes; por tal motivo, su aplicación no obedece a un orden estricto, sino al desarrollo y los requerimientos generados.

[3-6] De un indicio o una información de CI puede emprenderse cualquier tipo de actividad propia de la disciplina, y, como producto de esta, se podrá desplegar cualquier otro tipo de tareas de CI; obedece esto a la posibilidad de emplear todos los medios y los recursos disponibles cuando la operación así lo amerite y se encuentre dentro de los fines y los límites establecidos en la Ley Estatutaria 1621 de 2013. Por ejemplo, una actividad de recolección de información puede establecer un posible incidente de CI que requiere iniciar una averiguación de CI; o bien, durante el análisis de la información se identifica una posible ventaja que puede usarse como fuente para recolectar información.

3.2. COMPONENTES DE LAS OPERACIONES

[3-7] Las operaciones de CI tendrán unos componentes esenciales para su desarrollo:

- Componente directo
- Componentes de apoyo

[3-8] **El componente directo** es el que requiere de la recolección de información mediante el empleo de la disciplina de HUMINT. Este componente incluye actividades de inteligencia vigilancia y reconocimiento (ISR, por su sigla en inglés), y se denomina directo, debido a la exposición de los agentes al contacto con fuentes, organizaciones, agencias y distintos actores de la amenaza. El componente directo de las

CI

Contrainteligencia

HUMINT

Inteligencia humana

COMPONENTES DE LAS OPERACIONES DE CI

Componente directo

Componentes de apoyo

CI | Contrainteligencia

operaciones de CI es un tipo de inteligencia de única fuente, como se explica en el MFRE 2-0.

[3-9] Cabe aclarar que una actividad por sí sola no se constituye en una operación. Para comprender esto se deben tener en cuenta los siguientes ejemplos, que muestran las diferencias entre una actividad de CI y una operación de CI que emplee el componente directo, así:

- **Ejemplo 1 (actividad de contrainteligencia):** un agente de CI lleva a cabo un contacto con una fuente para obtener información acerca de un grupo de personas pertenecientes a la amenaza, y que estarían intentando subvertir la ideología de militares activos. Para el ejemplo descrito, esto corresponderá al empleo del componente directo para el desarrollo de una actividad de CI relacionada con contrasubversión.
- **Ejemplo 2 (operación de contrainteligencia):** el Batallón de Contrainteligencia Militar No. 2, despliega todas las capacidades de recolección de información hacia una zona fronteriza, a fin de identificar y contrarrestar un grupo de inteligencia extranjera que estaría desarrollando actividades de espionaje en territorio colombiano. Para el ejemplo descrito, esto es una operación de contraespionaje que emplea el componente directo.

FCG | Función de conducción de la guerra

[3-10] Por otro lado están los **componentes de apoyo**, los cuales se ejecutan a través de la FCG Inteligencia y suministran información para la ejecución de operaciones de inteligencia y CI y permiten el desarrollo de tareas de la FCG Protección mediante el empleo de técnicas y procedimientos enfocados a contribuir a la seguridad de personas, instalaciones e información reservada y clasificada de la Fuerza, para prevenir, detectar, negar o mitigar los riesgos y las amenazas actuales o potenciales de las estructuras de inteligencia enemiga.

[3-11] Estos componentes incluyen todas las actividades y las tareas desarrolladas por la competencia distintiva de la seguridad militar y sus funciones (seguridad de la información, seguridad de la infraestructura crítica, seguridad de personas y seguridad física), las cuales orientan sus labores a contribuir

con informaciones que sirvan a la CI para iniciar misiones de trabajo, confirmar o desvirtuar indicios de actividades irregulares o ilícitas en la Fuerza y proteger en todo caso los activos críticos del Ejército. Para ello se podrán emplear una o varias técnicas o procedimientos de distintas funciones de seguridad militar, a fin de que se permita solventar los vacíos de información relativos a un incidente de CI sobre el cual se desconocen, o aún no existen, indicios acerca de sus actores o sus responsables.

[3-12] Como ya se explicó, una actividad por sí sola no se constituye en una operación. En el caso de los componentes de apoyo, estos también pueden ser aplicados de forma independiente. Sin embargo, si se ejecutan de manera simultánea con un objetivo común, pueden constituirse en una operación sin interactuar o emplear el componente directo. Para comprender esto se deben tener en cuenta los siguientes ejemplos:

- **Ejemplo 1 (actividad de constrainteligencia):** se lleva a cabo un estudio diagnóstico de seguridad de rutas en respuesta a un requerimiento emitido por la primera división del Ejército: esto corresponde al empleo de un componente de apoyo para el desarrollo de una actividad relacionada con la seguridad de personas.
- **Ejemplo 2 (operación de constrainteligencia):** se materializa una fuga de información que compromete a distintas unidades adscritas a la Primera División, donde se requiere el empleo simultáneo de varias tareas tácticas de seguridad militar para identificar las causas, los efectos y a las personas implicadas en el incidente. Esto corresponde al empleo de los componentes de apoyo para el desarrollo de una operación de contraespionaje.

[3-13] De igual manera, una operación puede aplicar los dos tipos de componentes, al efectuar diferentes técnicas o procedimientos de la disciplina de CI, o apoyarse en las actividades de otras disciplinas de la FCG Inteligencia.

- **Ejemplo:** a través de la verificación de un estudio de seguridad de personal, se identifica que un miembro de la

CI

Contrainteligencia

FCG

Función de conducción de la guerra

institución, quien labora en el depósito de armamento de una división, se encuentra devengando menos del 70% de su salario, debido a diferentes descuentos realizados por nómina y sin otros ingresos adicionales, razón por la cual, a través de la sección de inteligencia de la unidad, se solicita un examen de poligrafía, mediante el que se obtiene información relacionada con el tráfico de material que se estaría presentado en el batallón. Esto motiva la entrega de la información a un batallón de contrainteligencia militar, el cual hace vigilancias y seguimientos que permiten identificar a los integrantes de la red, lo cual, tras el proceso pertinente de judicialización, conlleva su neutralización. Para el ejemplo descrito, esto corresponde a la integración del componente directo y el componente de apoyo durante el desarrollo de una operación de CI.

CI | Contrainteligencia

3.3. OPERACIONES DE CIBERCONTRAINTELIGENCIA

[3-14] Las ***operaciones de cibercontrainteligencia*** se definen como **acciones tácticas que permiten recolectar información de contrainteligencia, para identificar, analizar contrarrestar y neutralizar acciones de la amenaza en el ciberespacio**. Estas operaciones se basan en mecanismos digitales para recolectar, neutralizar o explotar una amenaza ya sea de espionaje, de sabotaje, de subversión o de terrorismo cibernetico.

[3-15] Las operaciones de cibercontrainteligencia (CCI) incluyen actividades de recolección en el ciberespacio centradas en amenazas de ciberterrorismo, inteligencia extranjera y amenazas emergentes que apuntan a los intereses nacionales e institucionales. Además de la recolección tradicional de CI, que se lleva a cabo usando fuentes técnicas y fuentes humanas, la recolección de datos en el ciberespacio se realiza principalmente a través de la red mundial (internet) para obtener información esencial que afecta a la operación apoyada. Esta puede resultar de averiguaciones o de operaciones de CI en curso, o bien, servir para iniciar una de ellas. El objetivo de la recolección de información en el ciberespacio es

proporcionar inteligencia de amenazas oportuna al comandante apoyado.

[3-16] Esta operación estará en capacidad de apoyar el procedimiento operacional de CI en cualquiera de sus pasos, dependiendo del ambiente operacional y del análisis y la evaluación que se deban realizar durante todo el proceso de inteligencia y el procedimiento operacional de CI.

CI

Contrainteligencia

3.4. PROCEDIMIENTOS DE CONTRAINTELIGENCIA

3.4.1 Procedimiento para el despliegue operacional de contrainteligencia

[3-17] La CI está organizada para apoyar los procesos de proyección de la fuerza mediante el despliegue de unidades, de personal y de material con el fin de:

- Apoyar las tareas asignadas a unidades militares en operaciones multinacionales.
- Cumplir requerimientos de información.
- Desarrollar operaciones de CI.
- Hacer parte de fuerzas multinacionales.
- Apoyar a las unidades territoriales con el fin de satisfacer los requerimientos de información y responder los RICC o los EEIPT.
- Dar cumplimiento a una misión de trabajo o a una orden de operaciones.

RICC

Requerimientos de información crítica del comandante

EEIPT

Elementos esenciales de información de las propias tropas

[3-18] Las unidades de CI operarán dentro de un área determinada, conforme a la misión asignada, y, en caso de ser requerido, podrá ser empleada en apoyo de una nación anfitriona, para contribuir a los objetivos de la acción decisiva. El despliegue operacional de CI se configura tomando en cuenta el empleo, la disposición y la ubicación del personal, de las

unidades y de los equipos de CI en relación con otras unidades, con el terreno y con el enemigo.

CI | Contrainteligencia

[3-19] En el ámbito de la CI se podrán presentar los siguientes escenarios de despliegue:

- **Escenario 1:** Despliegue de una unidad táctica en cumplimiento de la jurisdicción asignada en la orden de operaciones.
 - **Ejemplo:** el Batallón de Contrainteligencia Militar No. 1 se desplegará en la jurisdicción de la Primera División y tendrá su puesto de mando en la ciudad de Santa Marta.
- **Escenario 2:** Despliegue de unidades fundamentales a un área determinada en cumplimiento de una orden formal (orden de operaciones-misión de trabajo) emitida por la Unidad Operativa Mayor o Menor.
 - **Ejemplo:** se emite una orden para el despliegue de las compañías de recolección de información hacia la región del Catatumbo, Norte de Santander, donde se presentó un incidente de seguridad en zona fronteriza, el cual se considera de atención prioritaria. Para esta actividad el comandante determina que se desplieguen unidades que tengan la capacidad de desarrollar operaciones de CI y actividades de seguridad militar.
- **Escenario 3:** Despliegue de unidades fundamentales a un área determinada en apoyo a una nación anfitriona por orden del comandante del Ejército.
 - **Ejemplo:** una nación anfitriona que se encuentra en conflicto bélico con otro país considerado hostil solicita apoyo militar a los asociados de la AU, en concordancia con los acuerdos establecidos. Una vez aprobado dicho apoyo, mediante orden presidencial, el Ejército de Colombia proporciona los apoyos necesarios, dentro de los cuales se destinan unidades de CI.

AU | Acción unificada

- **Escenario 4:** Despliegue de agentes en cumplimiento de un requerimiento específico.
 - **Ejemplo:** el Batallón de Contrainteligencia Militar No. 1 despliega cinco agentes de CI para el cumplimiento de una actividad específica en un área determinada del territorio nacional.

[3-20] El procedimiento para el despliegue operacional de CI implicará la supervisión constante del mando superior, el cual deberá velar por la aplicación de las medidas de seguridad de los agentes, y ordenará, si es necesario, el repliegue de unidades o de personal en pro de mantener la integridad de los agentes, así como la continuidad de la operación o de las actividades desarrolladas en el área.

[3-21] Este procedimiento puede prolongarse en el tiempo, de acuerdo con la misión, la intención del comandante o las necesidades operacionales. Los pasos del procedimiento para el despliegue operacional de CI son:

- **Paso 1. Predespliegue:** esta actividad se lleva a cabo con el fin de efectuar un planeamiento previo al despliegue. Los comandantes de CI, apoyados por las secciones de inteligencia y de operaciones —y, si es necesario, por las secciones de personal y de logística— deben desarrollar las siguientes actividades:
 - **Analizar los requerimientos de información.** De acuerdo con el análisis de información y el análisis operacional ejecutado por las secciones de inteligencia y de operaciones de las unidades operativas, menores o tácticas de CI, se determinará la viabilidad del despliegue tomando en cuenta la misión y los objetivos de cada una de las unidades de CI. Una vez realizado el análisis, se aprobará o no el despliegue.
 - **Asignar unidades.** El comandante del nivel competente determinará cuáles son las unidades requeridas para el desarrollo de la actividad, averiguación u operación, con base en el análisis previo.

CI

Contrainteligencia

- **Preparar los recursos.** Las unidades comprometidas para el despliegue llevarán a cabo los trámites de índole administrativa a que haya lugar; asimismo, enfocarán sus esfuerzos en la preparación del personal para la aplicación de fachadas e historias del personaje en caso de que sea necesario. Además, se deberá realizar un estudio sociodemográfico del área en donde la unidad a ser desplegada llevará a cabo las actividades de CI. En este estudio se relacionará información acerca de los siguientes aspectos, entre otros:

- > Dinámica y estructura de la población.
- > Condiciones de vida.
- > Cultura.
- > Ciencia y tecnología.
- > Educación.
- > Economía.
- > Salud.

El estudio en mención deberá suministrar, además de los riesgos y las amenazas a los que estarían expuestos los agentes, las recomendaciones específicas y detalladas que en cada escenario correspondan, incluyendo fachadas e historias del personaje que se requieran. El estudio sociodemográfico será realizado como parte de las actividades de gestión operacional, y será llevado a cabo por la unidad destinada para tal fin, a la cual se le deberá suministrar la información requerida para que enfoquen el desarrollo de sus análisis a los lugares críticos del área determinada para la labor de CI.

- **Emitir órdenes e instrucciones.** Las órdenes e instrucciones deberán ser emitidas mediante una orden de operaciones o una misión de trabajo, según corresponda. Estos documentos deberán contener

órdenes específicas en relación con los siguientes aspectos:

- Información por recolectar.
- Medidas de seguridad.
- Misión por cumplir.
- Canales de comunicación.
- Mando de la misión.
- Agregaciones o segregaciones.
- Todas las demás órdenes e instrucciones que el comandante estime convenientes.
- **Paso 2. Despliegue:** se define como *despliegue* el movimiento de fuerzas y material desde su punto de origen hasta un área de operaciones (MFRE 2-0). En este paso se efectuarán los movimientos pertinentes ubicando al personal en los puntos y en las áreas establecidas en el primer paso del procedimiento. Durante el despliegue, las unidades de CI deben cumplir las siguientes actividades:
 - Reducir vacíos de información.
 - Emitir alertas.
 - Identificar vulnerabilidades.
 - Establecer enlaces.
- **Paso 3. Empleo de las unidades:** durante el despliegue, la unidad o las unidades de CI deberán cumplir las tareas específicas de recolección de información plasmadas en la orden de operaciones o misión de trabajo. Dichas tareas dependerán, en gran medida, del objetivo del despliegue; sin embargo, se deberán cumplir algunas tareas complementarias, tales como:
 - Apoyar la FCG Inteligencia para responder los RICC o los EEIPT.
 - Responder los requerimientos de información.

CI | Contra Inteligencia

FCG	Función de conducción de la guerra
RICC	Requerimientos de información crítica del comandante
EEIPT	Elementos esenciales de información de las propias tropas

- Apoyar las operaciones militares.
- Confirmar o desvirtuar información.
- Hacer parte de una fuerza multinacional.
- **Paso 4. Evaluación periódica sobre continuidad del despliegue:** se deberá hacer una evaluación periódica tanto del nivel de riesgo al que se hallan expuestos los agentes, como de los avances y de la producción de CI obtenida en el cumplimiento de las actividades.
- **Paso 5. Repliegue de unidades:** una vez cumplida la misión, o por orden del comandante, se llevará a cabo el repliegue del personal o de las unidades. Esto se hará cumpliendo todas las medidas de seguridad, y se evaluará, si es necesario, un *redespliegue* entendido como el proceso por el cual las unidades y el material se reposicionan en la misma área de operaciones (MFRE 2-0).

3.4.2 Procedimiento para la integración de actividades en un área específica

CI

Contrainteligencia

[3-22] La CI dispone de unidades que cumplen tareas diferenciales, las cuales pueden encontrarse distribuidas en una misma área cumpliendo con el desarrollo de las actividades propias asociadas a su misionalidad. Ello implica que, en el territorio nacional, cada una de las divisiones del Ejército cuente con el apoyo de unidades de CI, que llevan a cabo sus actividades de manera independiente y en apoyo de las unidades territoriales que se encuentran dentro del área específica de una división.

[3-23] Sin embargo, en algunos escenarios que se encuentran condicionados a la situación operacional y a los requerimientos de información, se necesitará de la integración y la sincronización de tareas o actividades de CI. Esta sincronización tiene por objetivo maximizar la efectividad de las operaciones mediante la integración de la información obtenida por cada una de las unidades de CI y fortalecer la producción de análisis dentro del área de operaciones de una división, al generar

estrategias y determinar las tareas clave para el cumplimiento de la misión, las cuales, a su vez, deberán desarrollarse implicando una retroalimentación permanente y completa que permita orientar y estipular los objetivos o los aspectos específicos en los cuales se deberá enfocar el esfuerzo de recolección de información.

[3-24] En consecuencia, este procedimiento tiene como finalidad integrar, cuando sea necesario y de acuerdo con la intención del comandante, las actividades de cada una de las unidades de CI que se encuentran dentro del área de operaciones de una misma división, estableciendo canales de comunicación, apoyos de otras funciones de CI y los parámetros para la coordinación necesarios para la articulación de actividades en un área determinada.

[3-25] La necesidad del empleo de este procedimiento podrá surgir por informaciones iniciales disponibles, obtenidas de tres formas:

- a. Solicitud de la unidad territorial por un incidente que requiera de la intervención de la CI.
 - b. Informe de contrainteligencia generado por el CI2CM en donde se demuestre la necesidad de la actividad focalizada de la CI.
 - c. Por una orden del comando superior donde se reciba información sobre la necesidad inminente del apoyo de CI en el área.
- **Paso 1. Estructurar la información disponible:** el CI2CM deberá complementar la información disponible o allegada empleando los medios humanos y técnicos disponibles, así como generando solicitudes de información a las unidades subordinadas, con el fin de determinar un blanco o un objetivo específico sobre el cual se va a dirigir la actividad de CI en el área, y teniendo en consideración los criterios y las órdenes emitidas por el comandante, con el propósito de integrar las capacidades disponibles en el área o el despliegue de las unidades fundamentales o de los agentes requeridos para cumplir la misión.

CI

Contrainteligencia

CI2CM

Centro Integrado
de Información de
Contrainteligencia
Militar

- **Paso 2. Determinar unidades comprometidas, servicios técnicos requeridos y otras actividades:** además de determinar las unidades fundamentales o los agentes requeridos para el cumplimiento de la misión, se deberán estipular los servicios técnicos de CI (ver el capítulo 6) o cualquier otra actividad de CI, como los procedimientos y las técnicas específicas que sean pertinentes, considerando las necesidades previstas y las que, conforme a un análisis prospectivo, puedan requerirse para la operación. En caso de que la actividad que se está llevando a cabo localmente requiera las capacidades de una unidad que no se encuentre dentro del mismo teatro de operaciones, esta unidad deberá implementar el procedimiento para el despliegue operacional de CI.
- **Paso 3. Emitir el plan de trabajo y las misiones de trabajo:** la sección de operaciones en coordinación con la sección de inteligencia de la unidad operativa mayor elaborará una orden de operaciones en donde se emitirán órdenes e instrucciones y se establecerán de manera detallada las funciones y las responsabilidades de cada una de las unidades comprometidas en la operación.

CI | Contrainteligencia

Posteriormente, el comandante al que le sean asignadas las unidades deberá emitir la misión de trabajo, y conforme a esta emitir las respectivas misiones de trabajo que soporten el desarrollo de las actividades. El desarrollo de las actividades de CI dentro de un área específica requiere una capacidad de análisis, para esto, por medio de la orden de operaciones se ordenará la integración de las capacidades de análisis de cada una de las unidades comprometidas en la operación.

- **Paso 4. Ejecutar las actividades:** cada una de las unidades comprometidas en la operación desarrollará las actividades que le fueron asignadas en la orden de operaciones, teniendo en cuenta las capacidades diferenciales de cada una.

- **Paso 5. Elaborar los informes finales de resultado:** como producto de las actividades desarrolladas se deberán efectuar dos tipos de informe final de resultados, así:
 - Informe de Constrainteligencia (externo) (ver el anexo A).
 - Informe de Constrainteligencia (interno) (ver el anexo A).

3.4.3 Procedimiento operacional de constrainteligencia

[3-26] Todas las competencias distintivas y las funciones pertenecientes a la disciplina de CI deberán aportar al procedimiento operacional de CI, ya que cada una de las anteriormente nombradas tiene capacidades diferenciales que aportarán durante el proceso con información, inteligencia o análisis, a fin de que el resultado de las operaciones de CI sea el más acertado posible.

[3-27] Este procedimiento tiene por objetivo consignar las actividades de CI realizadas, para lograr fortalecer con información las bases de datos de CI, responder los RICC y los EEIPT, aportando al PMTD y garantizando el registro y control de las actividades de CI, efectuadas por unidades encubiertas que adelanten averiguaciones u operaciones de la disciplina.

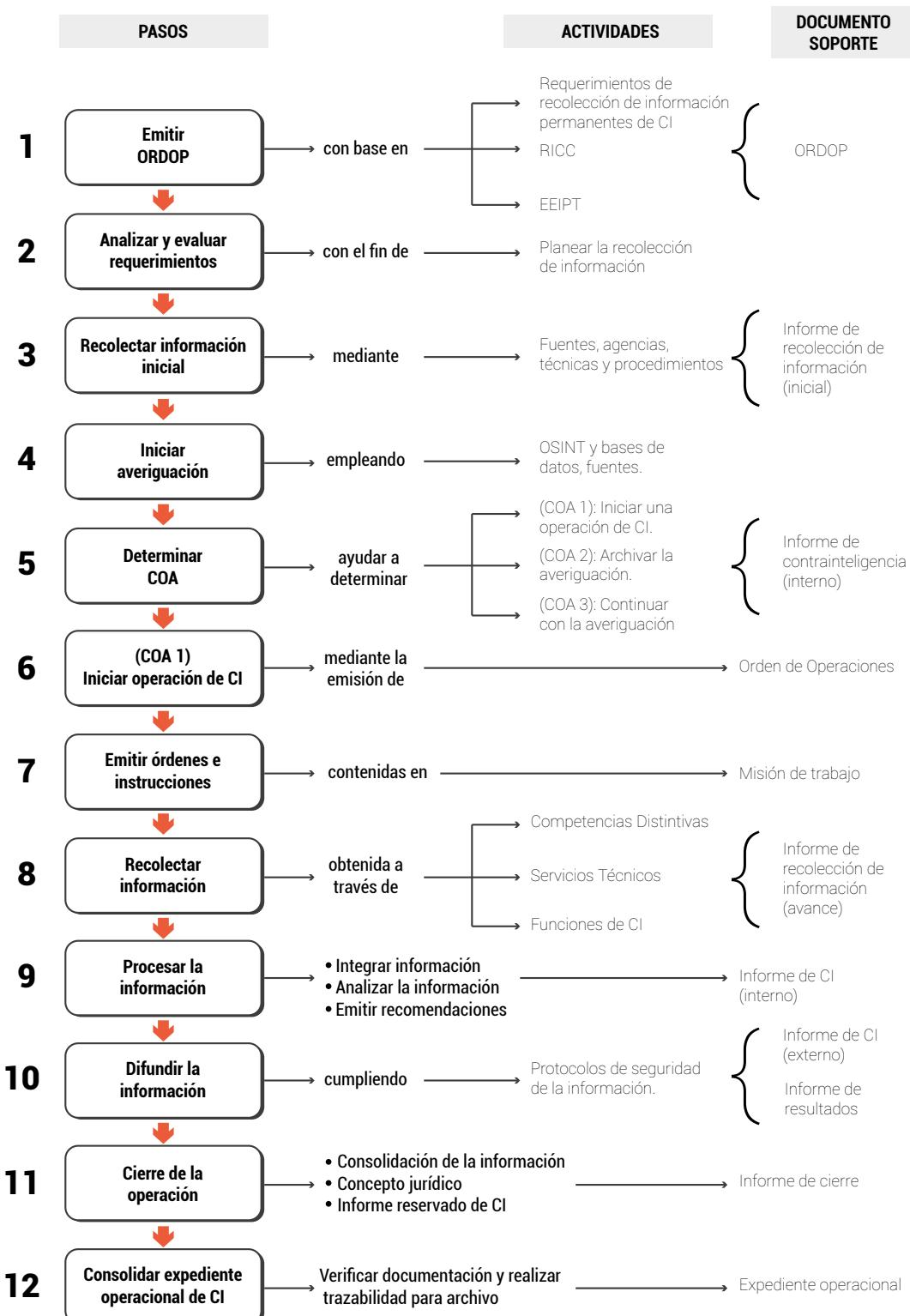
[3-28] El procedimiento operacional de constrainteligencia describe la secuencia de las actividades por desarrollar para hacer una averiguación o una operación de CI, así:

CI | Constrainteligencia

RICC | Requerimientos de información crítica del comandante

EEIPT | Elementos esenciales de información de las propias tropas

PMTD | Proceso militar para la toma de decisiones



| Figura 3-1 | Procedimiento operacional de contrainteligencia

Paso 1. Emitir orden de operaciones

[3-29] La *orden de operaciones* es una directriz emitida por un comandante a sus comandantes subordinados con el propósito de coordinar efectivamente la ejecución de una operación (MFE 1-01). Esta se constituye en un documento de soporte de las actividades de CI; su planeación y su desarrollo se enmarcan en el cumplimiento de las disposiciones contenidas en la Ley 1621 del 17 de abril de 2013, y su contenido y sus elementos básicos se encuentran estipulados en el artículo 2.2.3.4.3 del Decreto Reglamentario 1070 de 2015.

CI | Contrainteligencia

[3-30] Para la emisión de la orden de operaciones se deben tener en cuenta los siguientes requerimientos.

Requerimientos de recolección de información permanentes de contrainteligencia

[3-31] La CI del Ejército, dentro de los límites de su misión, de las prioridades asignadas, de los recursos, de la ubicación y de la capacidad de recolección, tiene la obligación de recoger e informar las siguientes categorías de información:

- Actividades de las redes de inteligencia de la amenaza.
- Incidentes de CI. Evento de conocimiento público relacionado con las acciones de inteligencia de la amenaza que se hayan materializado, y las cuales afectan o afectarán al Ejército o a los asociados de la AU.
- **Indicios de contrainteligencia. Información inicial que de acuerdo con el análisis de contrainteligencia podría representar una posible acción de la inteligencia de la amenaza.**
- Acciones de la amenaza conocidas o sospechosas (sabotaje, subversión, espionaje, terrorismo, insurgencia o corrupción).
- Cualquier información de interés para la CI.

AU | Acción unificada

Requerimientos de información crítica del comandante (RICC)

[3-32] *Requerimientos de información crítica del comandante* se definen como requerimiento de información identificado por el comandante como crítico para facilitar una toma de decisiones oportuna (MFRE 2-0). Estos requerimientos deben ser respondidos al comandante militar, y, usualmente, obedecen a vacíos de información en uno o varios de los factores relevantes del ambiente operacional identificados antes o durante del desarrollo de operaciones militares; esto, para cumplir de manera efectiva la misión asignada.

Elementos esenciales de información de las propias tropas (EEIPT)

[3-33] *Elementos de esenciales de información de las propias tropas* definidos como aspectos críticos de la operación de las propias tropas que de ser conocidos por el enemigo comprometerían, llevarían al fracaso o limitarían el éxito de la operación; por lo tanto, deben ser protegidos de la detección por parte de este (MFRE 2-0).

CI

Contrainteligencia

[3-34] Una de las prioridades del comandante es proteger al personal, la información, los recursos, los medios y la infraestructura de las propias tropas. Por lo tanto, la CI recolecta información acerca de dichos elementos o activos críticos del Ejército para recomendar al comandante cursos de acción en cualquier etapa de la operación con el fin de negarle al enemigo información que comprometería la supervivencia de la operación o de las propias tropas.

Paso 2. Analizar y evaluar requerimientos

[3-35] Los agentes de CI deben conocer los documentos plasmados en el paso 1 del presente procedimiento, con el fin de recolectar información acerca de esos requerimientos de información. Aunque existen requerimientos de información que son específicos, hasta este paso aún no se tiene una

información puntual sobre las actividades de inteligencia de la amenaza; se debe propender por verificar desde este paso si la información es falsa o no segura, a fin de proteger a los agentes y evitar el desgaste operacional.

[3-36] El comandante, tomando en cuenta los requerimientos de información planteados, los planes operacionales de la unidad operativa mayor, la orden de operaciones de la unidad operativa menor, y la orden de operaciones de la unidad táctica, se organiza tácticamente en el AO con el fin de obtener una información inicial que pueda servir de base para el inicio de una averiguación.

[3-37] Para este planeamiento se deberá tener en cuenta:

- Análisis previo de la información disponible.
- Análisis de la información por recolectar.
- Aspectos del ambiente operacional.
- Aspectos de seguridad.
- Medios con lo que se cuenta para obtener la información.
- Conocimiento de los procedimientos y de las técnicas que se van a implementar.
- Otros aspectos que el comandante estime convenientes.

AO	Área de operaciones
CI	Contrainteligencia

Paso 3. Recolectar la información inicial

[3-38] La información inicial de CI es un conjunto de datos de interés para la CI. Puede ser obtenida por diferentes canales de difusión (del comando, del estado mayor, de técnicos), así como puede ser recolectada por fuentes, agentes de CI o medios de recolección de información (humanos o técnicos). Asimismo, existen otras fuentes que podrán aportar información, sin ser las únicas:

- Operaciones de CI que suministren información acerca de otros objetivos que no puedan ser trabajados dentro de la misma operación de CI.

FCG

Función de
conducción de la
guerra

- Actividades de recolección de información en el ciberespacio.
- Contacto con fuentes humanas.
- Informes de las disciplinas de la FCG Inteligencia.
- Analistas operacionales.
- Procedimiento de contraespionaje del equipo rojo.
- Apoyos de CI.
- Entrevistas de CI.

[3-39] Los agentes y las unidades encargadas de adelantar técnicas y procedimientos propios de las funciones y las competencias distintivas de CI deberán expresar por escrito, a través de un informe de recolección de información (inicial) (ver el anexo B), la información de interés recibida, y este será el único documento que podrá dar inicio a una averiguación de CI.

CI

Contrainteligencia

CI2CM

Centro Integrado
de Información de
Contrainteligencia
Militar

[3-40] La unidad táctica enviará el informe de recolección de información, mediante oficio remisorio, a la sección de análisis del Centro Integrado de Información de CI Militar (CI2CM) o quien haga sus veces, por cuanto este posee las bases de datos de CI y cuenta con capacidades de recolección y de análisis mayores que las de las unidades tácticas. Este informe deberá especificar los requerimientos de información que serán respondidos por el CI2CM.

[3-41] **Informe de recolección de información (inicial):** este documento se convierte en la base para iniciar una averiguación o una operación de CI. La información consignada en este documento es el resultado de la recolección de información de los agentes de CI, por cualquier medio. Esta recolección se hace de forma general, ya que muchas veces no obedece a un requerimiento de información específico, planteado en una misión de trabajo, sino que obedece al trabajo rutinario de los agentes de CI, que permanentemente deben estar recolectando información de CI, debido a la naturaleza de su oficio.

[3-42] La información inicial, normalmente, no obedece a un proceso complejo de análisis ni de tratamiento de la información, ya que dicho proceso vendrá en el desarrollo de las averiguaciones o las operaciones de CI. Asimismo, esta información puede ser resultado de una charla informal, de un sondacamiento, de la motivación de una persona para brindar información, de un anónimo, etc. Estos son los ítems que debe tener este tipo de informe:

- Receptor de la información.
- Marco operacional.
- Procedencia de la información. Se debe consignar mediante qué medio fue obtenida la información inicial; por ejemplo: exámenes de credibilidad y confiabilidad, fuente humana, canales de estado mayor, comando o técnicos, medios técnicos, actividades de seguridad militar, entrevistas, otros.
- Información recolectada. Se deben plasmar todos los datos y la información recolectada; esta información va desde un alias o una fotografía hasta transcripciones de conversaciones o datos poligráficos. El agente no podrá omitir ningún detalle de la información inicial, ya que esta se convertirá en la base de una averiguación de CI o de una operación de CI. Asimismo, el agente le debe dar una evaluación a la fuente (en caso de que sea fuente humana) y a la clasificación de la información. Esta información podrá ser evaluada cuando se realicen procesos más complejos de análisis.
- Recomendación. El agente deberá consignar todas las observaciones que tenga en cuanto a la información y la fuente de información. Asimismo, deberá emitir recomendaciones de cursos de acción para la recolección de información futura.
- Asuntos administrativos.
- Pertinencia. Consignar a quién es pertinente la información recolectada.

CI

Contrainteligencia

MRI	Medios de recolección de información
FCG	Función de conducción de la guerra
CI	Contrainteligencia
CI2CM	Centro Integrado de Información de Contrainteligencia Militar

Paso 4. Iniciar averiguación

[3-43] Las **averiguaciones** se definen como la **actividad de contrainteligencia enfocada a confirmar o desvirtuar los indicadores de los incidentes de seguridad**. Las averiguaciones de CI se realizan cuando se identifican posibles indicadores, incidentes o información de CI suministrada por los MRI y es plasmada en un informe de recolección de información. Las averiguaciones se llevan a cabo para detectar, identificar, explotar y neutralizar la inteligencia extranjera y los servicios de seguridad (FISS, por su sigla en inglés), las organizaciones terroristas (OT), agentes locales y otras amenazas. El objetivo de las averiguaciones de CI es establecer la veracidad de la información consignada en el informe de recolección de información (initial).

[3-44] Las averiguaciones de CI explotan la información inicial ampliando dicha información mediante el apoyo de una o más disciplinas de la FCG Inteligencia y el uso de los siguientes medios, sin ser estos los únicos:

- Consulta de base de datos de CI y antecedentes poligráficos.
- Consulta de bases de datos obtenidas a través de convenios interinstitucionales (registraduría, unidad de información y análisis financiero, policía, etc.)
- Consulta en base de datos de la comunidad de inteligencia y contrainteligencia.

[3-45] Esta actividad debe realizarla el Centro Integrado de Información de Contrainteligencia Militar (CI2CM) o quien haga sus veces, teniendo en cuenta que es vital hacerla oportunamente, por lo cual las consultas deben realizarse con celeridad y sin dilación. El CI2CM, al poseer la información, es responsable de su uso y de su custodia.

[3-46] Como resultado de estas consultas, el Centro Integrado de Información de Contrainteligencia Militar (CI2CM) deberá elaborar un informe de contrainteligencia (ver el anexo A),

donde se especifique toda la información recolectada, incluyendo fotografías, direcciones o cualquier dato de interés.

[3-47] **Informe de CI (interno):** la finalidad de este informe es ampliar la información inicial empleando otros MRI, con el objeto de recolectar la mayor cantidad posible de datos mediante un análisis más detallado, y poder tomar decisiones acerca del inicio de una operación de CI. Los ítems que debe tener este tipo de informe son:

- Receptor.
- Marco operacional.
- Enemigo o amenaza: se deben consignar todos los datos del enemigo, la amenaza o la fenomenología criminal, según sea el caso.
- Información recolectada: se debe registrar la totalidad de la información recolectada, tomando en cuenta datos como direcciones, identidad, correos electrónicos, antecedentes, fotografías o cualquier otra información de interés que potencialice la futura operación de CI.
- Análisis: de acuerdo con la información inicial recolectada a través de las funciones de la CI o de los servicios técnicos, se le deben aplicar a esta las matrices, los diagramas, la interconexión de información o cualquier tipo de técnicas de análisis de información que logren refinar los datos obtenidos para concluir los posibles cursos de acción.
- Recomendaciones: determinar los cursos de acción para iniciar una operación de CI, archivar la información obtenida en la base de datos o continuar con las averiguaciones.
- Pertinencia.
- Anexo: se debe anexar, en medio digital o físico, la información de interés que no se haya plasmado en el informe, ejemplo: información digital que, por su tamaño, no debe ser impresa dentro del cuerpo del informe; también,

MRI | Medios de recolección de información

CI | Contrainteligencia

fotografías, croquis, mapas o planos, que pueden ser visualizados de una mejor manera a través de medios digitales, información obtenida mediante el monitoreo del espectro electromagnético e información poligráfica.

Paso 5. Determinar curso de acción

CI2CM Centro Integrado de Información de Contrainteligencia Militar

[3-48] El informe de CI desarrollado por el CI2CM deberá ser enviado al comandante de la Unidad Táctica de CI al que sea pertinente la información. El comandante, mediante el análisis y la evaluación de la información suministrada, deberá determinar uno de los siguientes cursos de acción:

- Curso de acción 1 (COA 1): iniciar una operación de CI.
- Curso de acción 2 (COA 2): archivar la averiguación. Debe usar el formato de cierre de misiones omitiendo el cierre jurídico.
- Curso de acción 3 (COA 3): continuar con la averiguación; en caso de ser seleccionado el COA 3, la duración máxima para darle inicio a una operación o para archivarla no podrá ser superior a un mes.

COA Curso de acción

CI Contrainteligencia

Paso 6. Iniciar operación de contrainteligencia

[3-49] Las operaciones de CI se desarrollan a partir del resultado de una averiguación realizada a través de fuentes abiertas y bases de datos, como se describe en el paso 4 del presente procedimiento, y la operación emplea las técnicas y los procedimientos necesarios para el cumplimiento del objetivo trazado. El documento para iniciar una operación de CI es una orden de operaciones determinando el objetivo específico de esta, y mediante la cual se deberá informar por escrito al comando superior acerca del inicio de la operación de CI.

[3-50] Para la elaboración de la orden de operaciones se debe tener en cuenta que esta:

- Debe ir orientada a cumplir el objetivo de la operación; es decir, es más específica que la orden de operaciones de la Unidad Táctica.
- Debe obedecer a un planeamiento entre el comandante, el oficial de operaciones y el oficial de inteligencia.
- Servirá de amparo para todas las actividades y las misiones de trabajo que se desprendan de ella.

Paso 7. Emitir órdenes e instrucciones

CI

Contrainteligencia

[3-51] Las órdenes e instrucciones de recolección de información deben ser emitidas a través de una **misión de trabajo**, definida como el **documento legal que regula las actividades de inteligencia y contrainteligencia, emitido por los directores de los organismos o jefes de unidad, sección o dependencia**. Esta se constituye en un documento soporte de las actividades de CI, su planeación y su desarrollo se enmarcan en el cumplimiento de las disposiciones de la Ley 1621 del 17 de abril de 2013 artículo 14 y del Decreto Reglamentario 1070 de 2015 artículo 2.2.3.4.3.

[3-52] Se deben emitir tantas misiones de trabajo como sean necesarias para dar cumplimiento a la orden de operaciones; en esta se debe aclarar qué información específica se necesita recolectar, así como las técnicas y los procedimientos por medio de los cuales se debe hacer dicha recolección.

Paso 8. Ejecutar la recolección de información

[3-53] La recolección de información debe estar basada en las misiones de trabajo y la orden de operaciones. Para la recolección de información, los agentes de CI contarán con las siguientes herramientas, sin ser estas las únicas:

- Plan de recolección de información.
- Coordinaciones con otras agencias o autoridades judiciales.

- Administración de fuentes e informantes.
- Servicios técnicos de CI.
- Información proveniente de las respuestas de las diferentes unidades que desarrollen competencias distintivas, técnicas y procedimientos de CI, de acuerdo con los requerimientos de información emitidos.

[3-54] Asimismo, esta actividad se puede realizar bajo la figura de agente encubierto con amparo judicial dentro de un proceso jurídico para obtener información que ayude a esclarecer un acto presuntamente delictivo. Los agentes podrán disponer de una o varias herramientas para recolectar información, según la necesidad.

[3-55] Como resultado de las actividades de recolección, y en concordancia con la misión de trabajo, se deberán rendir los correspondientes informes de recolección de información.

[3-56] **Informe de recolección de información (avance)** (ver el anexo B): en este documento se debe plasmar la información recolectada por los agentes de CI, en concordancia con los requerimientos de información específicos ordenados en la misión de trabajo. Los siguientes son los ítems que debe tener este tipo de informe:

- Receptor.
- Marco operacional.
- Tiempo empleado.
- Información recolectada.
- Recomendaciones: el responsable de la misión debe consignar recomendaciones respecto a la fuente, la información, los vacíos de información y las proyecciones de recolección de información.
- Asuntos administrativos: relacionar los recursos que se emplearon para recolectar la información, incluyendo el

pago de información a fuentes tomando en cuenta la normatividad vigente de gastos reservados.

Paso 9. Procesar la información

[3-57] El *procesamiento* es el desarrollo de la inteligencia a través del análisis de la información recolectada y de la inteligencia existente (MFRE 2-0).

[3-58] Los analistas de inteligencia y CI tienen a su disposición grandes volúmenes de información producto de operaciones, competencias distintivas, funciones de CI, otras disciplinas de la FCG Inteligencia y otras fuentes de información. Estos analistas reciben la información recolectada durante la operación de CI, y posteriormente la clasifican para su procesamiento.

[3-59] De acuerdo con la clasificación, los analistas integran la información de todas las fuentes para tener mayores criterios de evaluación y refinar los productos de CI.

[3-60] De esa forma, el analista logrará facilitar el entendimiento de la información y apoyar a la toma de decisiones para recomendar el siguiente paso dentro del proceso, ya sea difundir la información o recomendar los requerimientos de información para su recolección.

[3-61] Como resultado del procesamiento de toda la información recolectada, se debe elaborar un informe de CI (interno) (ver el anexo A), donde se le da cumplimiento a la orden de operaciones y se finaliza la recolección de información.

Paso 10. Difusión de la información

[3-62] Teniendo el resultado de la recolección de información plasmada en el informe de CI y las recomendaciones, se pueden tomar las siguientes decisiones:

- Dar por culminada la operación y archivar, debido a que no se pudo confirmar la información inicial.

CI	Contrainteligencia
FCG	Función de conducción de la guerra

RICC	Requerimientos de información crítica del comandante
EEIPT	Elementos esenciales de información de las propias tropas
AU	Acción unificada
CI	Contrainteligencia

- Neutralizar la amenaza, ya sea por medios militares, por actividades de CI o con la colaboración de los entes judiciales.
- Difundir información para responder los RICC o los EEIPT, o bien, para la toma de decisiones.
- Archivar la información para su futura consulta.

[3-63] En caso de que se decida difundir la información de CI, se debe elaborar un informe de CI (externo), que podrá ir dirigido a los asociados de la AU, a las unidades militares o a otras agencias de inteligencia o CI, dependiendo del tipo de información y de la clasificación de esta, el mencionado documento podrá ser difundido, tomando en consideración la respuesta a los siguientes interrogantes, para aportar a la toma de decisiones:

- ¿A quién es pertinente la información?
- ¿La información se constituye en insumo para realizar una operación militar?
- ¿A quién puede dirigirse la difusión de la información, de acuerdo con su sensibilidad?
- ¿Con qué finalidad se difunde el informe?

[3-64] **Informe de Contrainteligencia (externo)** (ver el anexo A): documento elaborado con el fin de difundir información de CI a entes distintos de los que hacen parte del Comando de Apoyo de Combate de contrainteligencia Militar o de quien haga sus veces. Este busca puntualizar sobre la inteligencia resultante de toda la operación de CI para que un líder pueda tomar decisiones acertadas. Los siguientes son los ítems que debe tener este tipo de informe:

- Receptor.
- Enemigo o amenaza.
- Información recolectada. Se debe evaluar la información.
- Análisis.
- Recomendaciones.



NOTA

En caso de que el resultado de la operación haya sido tangible, se debe anexar el informe de resultados.

[3-65] **Resultados operacionales:** mediante un informe de resultados (ver el anexo C), se plasman todos los aspectos relacionados con el resultado operacional de CI. Dicho documento se convierte en la base para analizar y evaluar la continuidad o el cierre de la misión. Puede existir más de un resultado en un expediente operacional. Los siguientes son los ítems que debe tener este tipo de informe:

- Receptor.
- Fecha.
- Ubicación.
- Tipo de operación.
- Resultado.

CI

Contrainteligencia

Paso 11. Cierre de la operación

[3-66] Teniendo en cuenta la decisión adoptada y el análisis previo de la no continuidad de la operación, se generará el cierre de esta; en tal virtud, se deberá elaborar el informe de cierre (ver el anexo D).

[3-67] **Informe de cierre:** documento basado en el análisis y la evaluación de la información, el cual contiene las actividades realizadas durante la operación de CI y determina el cierre de la operación. Asimismo, en este punto se debe determinar si las personas o las organizaciones que se relacionan durante el desarrollo de la operación deberán llevar registros reservados de CI. Los siguientes son los ítems que debe tener este tipo de informe:

- Receptor.
- Marco operacional.

- Enemigo o amenaza.
- Información recolectada.
- Acciones tomadas.
- Concepto jurídico.
- Conclusiones.

Paso 12. Consolidar el expediente operacional de contrainteligencia

[3-68] El expediente operacional es resultado documental de toda la operación de CI, y deberá contener los siguientes formatos, en el siguiente orden específico:

1. Orden de operaciones.
2. Informe de recolección de información (inicial).
3. Informe de CI (interno).
4. Orden de operaciones específica.
5. Misiones de trabajo (tantas como sean necesarias).
6. Informes de recolección (avance; tantos como sean necesarios, en concordancia con las misiones de trabajo).
7. Informe de CI (interno; paso 8).
8. Informe de CI (difusión, en caso de que se hubiera elaborado).
9. Informe de resultados (en caso de que se hubiera elaborado).
10. Informe de cierre.

CI | Contrainteligencia

[3-69] Este expediente deberá reposar en los archivos físicos y digitales de la unidad operativa mayor, a fin de que sirvan de insumo para futuras consultas.

OPERACIONES DE CONTRAINTELIGENCIA

Secuencia de acciones tácticas para la recolección de información sobre las acciones de inteligencia de la amenaza y los indicios de corrupción al interior de la Fuerza (MCE 2-22.1).

OPERACIONES DE CIBERCONTRAINTELIGENCIA

Acciones tácticas que permiten recolectar información de contrainteligencia, para identificar, analizar contrarrestar y neutralizar acciones de la amenaza en el ciberespacio (MCE 2-22.1).

INDICIOS DE CONTRAINTELIGENCIA

Información inicial que de acuerdo con el análisis de contrainteligencia podría representar una posible acción de la inteligencia de la amenaza (MCE 2-22.1).

AVERIGUACIONES

Actividad de contrainteligencia enfocada a confirmar o desvirtuar los indicadores de los incidentes de seguridad (MCE 2-22.1).

MISIÓN DE TRABAJO

Documento legal que regula las actividades de inteligencia y contrainteligencia, emitido por los directores de los organismos o jefes de unidad, sección o dependencia (MCE 2-22.1).

PRODOP	Proceso de operaciones
RICC	Requerimientos de información crítica del comandante
EEIPT	Elementos esenciales de información de las propias tropas
CI	Contrainteligencia
ORDOP	Orden de operaciones

3.4.3.1. El proceso de operaciones y el procedimiento operacional de contrainteligencia

[3-70] El proceso de operaciones (PRODOP) es una serie de pasos que el comandante desarrolla en las operaciones a través del mando tipo misión: planear, preparar, ejecutar y evaluar (MFE 5-0). A continuación, se enumera cómo el procedimiento operacional de CI se encuentra alineado con el PRODOP.

[3-71] *Planear* es el arte y la ciencia de entender una situación de manera prospectiva para visualizar el futuro deseado y trazar formas eficaces a fin de conseguirlo (MFE 5-0). Para impulsar el proceso de operaciones, los comandantes conducen este proceso a través del entendimiento, la visualización, la descripción, la dirección, el liderazgo y la evaluación de las operaciones. Para los comandantes de CI es relevante conocer aspectos importantes a fin de lograr emitir una ORDOP general, los cuales incluyen:

- Intención del comandante.
- Análisis y evaluación de los requerimientos (EEIPT, RICC, requerimientos de recolección permanentes de CI).

[3-72] Los mencionados aspectos implican que planear en el PRODOP enmarca los tres primeros pasos del proceso operacional de CI:

- Emitir ORDOP.
- Analizar y evaluar requerimientos.
- Recolectar información.

[3-73] Planear ayuda a los comandantes a crear y comunicar una visión común entre el comando, su estado mayor o plena mayor y sus subordinados, lo cual tiene como resultado un plan u orden que sincroniza la acción de las fuerzas en tiempo, espacio y propósito para alcanzar los objetivos y cumplir la misión.

[3-74] El proceso operacional de CI se sincroniza y se apoya mutuamente con las metodologías del planeamiento del Ejército, ya que esta puede complementar, dar respuesta o hacer parte de cualquiera de tres metodologías: la Metodología del diseño del Ejército, el Proceso militar para la toma de decisiones o el Procedimiento de comando.

[3-75] *Preparar* consiste en aquellas actividades realizadas por unidades y soldados para mejorar su capacidad de ejecutar una operación (MFE 5-0). En el caso de la CI, los agentes inician averiguaciones preliminares para determinar el mejor COA, el cual determinará si se inicia una operación de CI o si no se encontraron méritos dentro de la averiguación para ejecutarlo. Asimismo, esta actividad ayuda a las planas mayores y a los agentes de CI a entender la situación operacional, y se deben conducir las siguientes actividades, de acuerdo con el procedimiento operacional de CI:

- Iniciar averiguación.
- Determinar los COA.

[3-76] De la misma forma, durante el preparar también se podrán llevar a cabo actividades tales como:

- Establecer enlaces y adelantar coordinaciones.
- Continuar con la recolección de información.
- Ejecutar actividades relacionadas con el sostenimiento.
- Llevar a cabo *briefing* y *debriefing*.
- Conducir ensayos.
- Refinar el plan o las órdenes.

[3-77] *Ejecutar* es poner en acción el plan mediante la aplicación del poder de combate para el cumplimiento de la misión (MFE 5-0). Para una adecuada ejecución de la operación de CI, se deberán tener en cuenta: la toma de decisiones durante la ejecución, los puntos de decisión, las directrices para una ejecución efectiva, capturar y retener la iniciativa a través de

CI | Contrainteligencia

COA | Curso de acción

PRODOP | Proceso de operaciones

CI | Contrainteligencia

la acción y aceptar los riesgos prudentes; todas estas, actividades descritas en el MFE 5-0. En este paso del PRODOP, el procedimiento operacional de CI ejecuta las siguientes actividades:

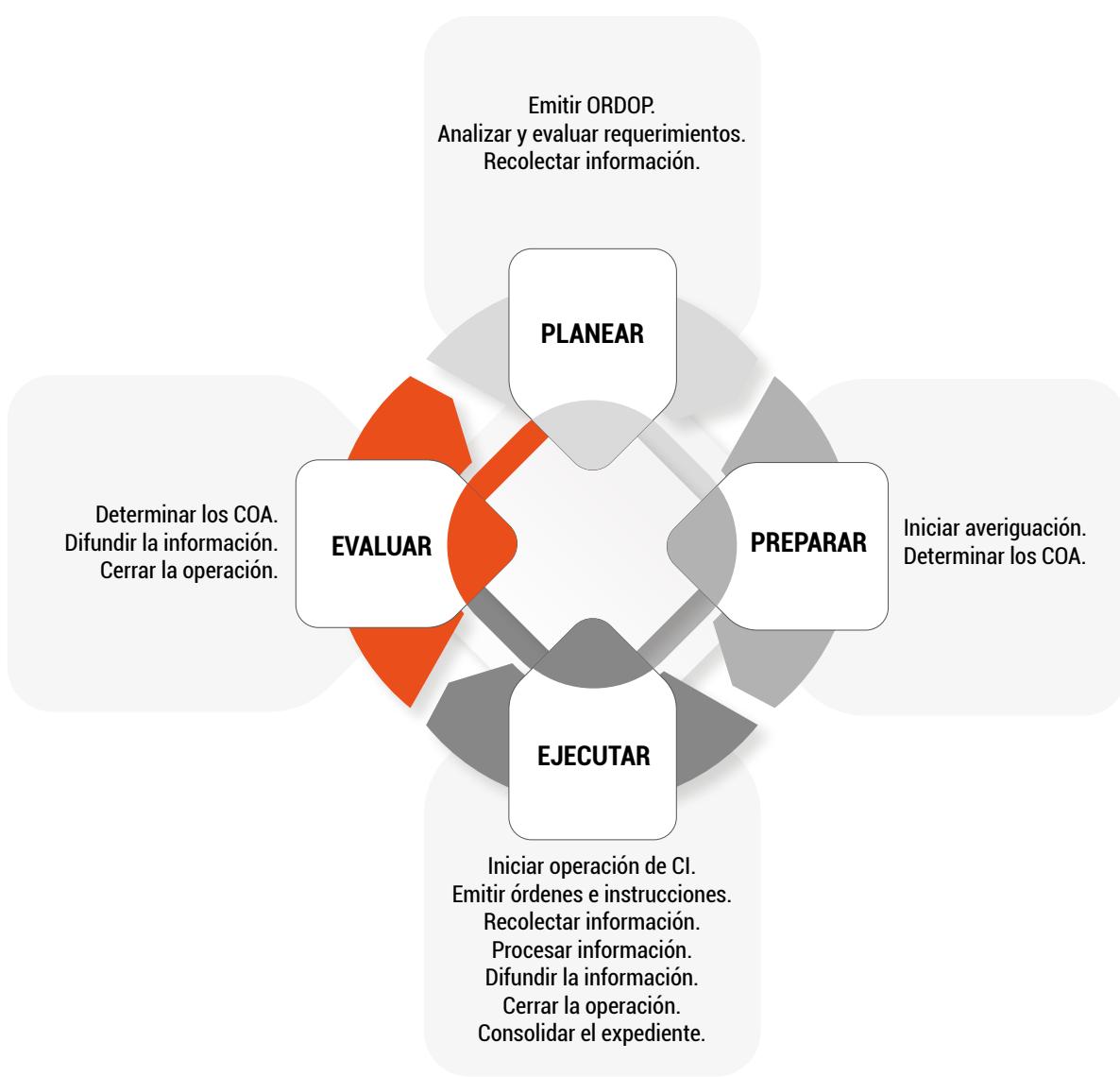
- Iniciar operación de CI.
- Emitir órdenes e instrucciones.
- Recolectar información.
- Procesar la información.
- Difundir la información.
- Cerrar la operación.
- Consolidar el expediente.

[3-78] *Evaluar* es medir el progreso en el cumplimiento de una tarea o misión, de la creación de un efecto o del logro de un objetivo (MFE 5-0). El procedimiento operacional de CI hace una evaluación constante durante el desarrollo de todo el proceso; sin embargo, existen tres momentos especiales donde el comandante debe llevar a cabo una evaluación más minuciosa aplicando cualquiera de las herramientas descritas en el MFRE 5-0. Estos momentos dentro del procedimiento son:

COA | Curso de acción

- Determinar los COA.
- Difusión de la información.
- Cierre de la operación.

[3-79] Finalmente, esta alineación se establece de forma gráfica, como se muestra en la figura 3-2.



| Figura 3-2 | Procedimiento operacional de contrainteligencia en el PRODOP

3.4.4. Procedimiento para asignación de analista de contrainteligencia

[3-80] Procedimiento por medio del cual se hace la asignación de un agente de CI a una unidad apoyada. Este agente realizará todos los enlaces de rutina; además, proporcionará asesoramiento y garantizará una familiarización detallada

con las operaciones, con base en los principios de compartimentación y reserva, y apoyará en la seguridad de la unidad identificando amenazas y vulnerabilidades, lo cual le permitirá, a su vez, recolectar información de interés para la CI. Los siguientes son los pasos que debe seguir la unidad táctica de CI para asignar a un analista de CI.

[3-81] El analista de CI asignado cumplirá órdenes e instrucciones de la unidad táctica de CI, de la cual es orgánico; por consiguiente, no podrá destinarse a otras actividades diferentes, así sean ordenadas por el comandante de la unidad apoyada, que se encuentren en contravía o fuera de lo establecido en la misión de trabajo.

[3-82] Este procedimiento se desarrollará en tres fases: antes, durante y después del despliegue, respectivamente. Cada fase comprenderá los siguientes pasos:

- Antes del despliegue: 1 al 3.
- Durante el despliegue: 4 al 7.
- Después del despliegue: 8 al 10.

CI | Contrainteligencia

AO | Área de operaciones

- **Paso 1.** Preparar al analista de CI en el conocimiento de las variables de la misión y las variables operacionales de la jurisdicción que se va a apoyar.
- **Paso 2.** Efectuar una prueba de conocimiento al analista acerca del AO de la unidad que se va a apoyar, para emitir un diagnóstico sobre el conocimiento y el grado de preparación del agente que permita emitir o no la autorización pertinente al despliegue.
- **Paso 3.** Desplegar al analista mediante una misión de trabajo (ver el anexo D del procedimiento operacional de CI), donde se especifiquen las funciones que va a desempeñar, la información que debe recolectar, las medidas de seguridad en el desarrollo del trabajo y otras instrucciones que se consideren necesarias para el cumplimiento de la misión.

- **Paso 4.** Brindar al comandante o al tomador de decisiones el conocimiento general del ambiente operacional de la jurisdicción respondiendo a las solicitudes de información (SI) relacionadas con EEIPT y con los RICC.
- **Paso 5.** Mantener relaciones profesionales basadas en la confianza, que permitan establecer vínculos propicios con los comandantes o los tomadores de decisiones y con todo el personal dentro y fuera de la unidad que pudiera colaborar con el suministro de información de CI para el desarrollo de averiguaciones o de operaciones; en lo posible, para la administración de fuentes de información.
- **Paso 6.** Cumplir las orientaciones de las actividades de recolección de información plasmadas en la misión de trabajo, tomando en cuenta las operaciones de CI que se estén desarrollando en la jurisdicción de la unidad apoyada; asimismo, informar al comandante directo acerca de las actividades llevadas a cabo en ese sentido.
- **Paso 7.** Dentro de su labor de CI, hacer seguimiento a las actividades de recolección de información y a las actividades rutinarias de la unidad asignada, con el fin de identificar o detectar oportunamente riesgos para la seguridad de las operaciones o para la propia unidad.
- **Paso 8.** Se debe hacer un *debriefing* que permita determinar la calidad de la labor desempeñada por el analista y proyectar las acciones de mejora necesarias para el cumplimiento de la misión.
- **Paso 9.** Una vez concluida la misión asignada, el analista deberá presentarse para la realización de su examen psicofisiológico de polígrafo, con el fin de evaluar aspectos relacionados con la seguridad de la información, los vínculos con personas al margen de la ley y cualquier otro aspecto que requiera ser evaluado, dada la actividad desarrollada por el agente.
- **Paso 10.** El analista debe entregar toda la información recolectada a los centros de análisis destinados para tal fin, con el objeto de someterla a las diferentes matrices.



ONG

Organización no gubernamental

[3-83] Los agentes de CI se podrán desempeñar como analistas para obtener información o hacer coordinaciones con organizaciones gubernamentales, o, bajo autorización, con ONG. La naturaleza de las actividades de CI y las numerosas restricciones legales impuestas hacen que la recolección de información de CI en tiempos de paz dependa, en gran medida, de un enlace efectivo.

[3-84] El analista asignado a las agencias militares y civiles es fundamental para el éxito de las operaciones de CI. En muchos casos, se hace necesario tener a analistas de tiempo completo para mantener un contacto regular con las organizaciones y las personas apropiadas.

[3-85] Un postulado básico para la actividad es el intercambio *quid pro quo* (algo por algo). Mientras que el agente de CI a veces se encuentra con individuos que cooperan debido a su sentido del deber o por razones desconocidas propias, el intercambio de información, de servicios o de material, u otro tipo de apoyo, normalmente forma parte de la interacción. La naturaleza de este intercambio varía ampliamente, dependiendo de la ubicación, la cultura y las personas involucradas. El espectro de tareas de enlace abarca desde el establecimiento de una buena relación con los empleados locales hasta la coordinación de operaciones multinacionales de las naciones aliadas. Los comandantes que tengan bajo su mando o su autoridad los enlaces deben tener en cuenta la realización de las siguientes actividades:

- Establecer los objetivos con los que se designa el enlace, así como las tareas que va a desarrollar dentro de la permanencia en el cargo.
- Determinar el tipo de información que se requiere recolectar.
- Establecer los canales de comunicación y la arquitectura de inteligencia necesaria para garantizar el flujo de información, con la seguridad requerida.

- Elaborar un plan de recolección específico, dentro del marco de la constitución y la ley para las operaciones conjuntas y multinacionales.
- Desarrollar los procedimientos operacionales estandarizados (SOP, por su sigla en inglés), que logren la cobertura total de las actividades relacionadas con las funciones que va a cumplir el analista.

[3-86] Los beneficios operacionales derivados de esta actividad incluyen:

- Establecimiento y fortalecimiento de relaciones laborales con las diferentes agencias, ejércitos, gobiernos, u otras organizaciones donde se encuentre un analista de CI.
- Organizar y coordinar operaciones conjuntas o multinacionales.
- Facilitar el intercambio de información de interés para las operaciones y la CI, que satisfagan los RICC o los EEIPT.
- Acceder a los registros reservados o públicos que de otro modo no estarían disponibles.

[3-87] Las limitaciones en esta actividad incluyen, entre otras:

- Restricciones acerca de la recolección de información de blancos específicos (personas u organizaciones).
- El personal que se utilice como enlace no podrá desarrollar actividades de forma encubierta hacia la organización, la jurisdicción o la zona donde sus miembros se desempeñan como analista.

[3-88] El agente de CI también debe comprender las capacidades de las agencias en las cuales se desempeña como analista. El conocimiento de las capacidades en términos de misión, recursos humanos, equipamiento y capacitación es esencial antes de solicitar información o servicios. La información intercambiada por el analista deberá ser sometida al proceso de inteligencia, con el fin de eliminar la información que no se requiere, la que puede estar manipulada o la que

CI | Contra Inteligencia

RICC | Requerimientos de información crítica del comandante

EEIPT | Elementos esenciales de información de las propias tropas

puede causar un desvío en la focalización de las actividades de CI.

[3-89] El agente de CI deberá observar y analizar el comportamiento de los nativos a fin de familiarizarse con su entorno y adaptarse a sus hábitos.

[3-90] Es posible que el agente de CI tenga que adaptarse a alimentos, bebidas, etiqueta, costumbres sociales y protocolos que desconocía. Las personas nativas esperan que un visitante oficial conozca las costumbres. El agente debe hacer un esfuerzo para evitar el choque cultural cuando se enfrenta a situaciones completamente ajena a sus propios antecedentes. El agente de CI debe lograr ajustarse a una amplia variedad de personalidades.

[3-91] Los registros y los informes son esenciales para mantener la continuidad de las actividades del analista, y deben tener la información precisa requerida y los objetivos previamente establecidos. Es preferible tener un archivo de cada organización o persona contactada, para, de esta forma, proporcionar una referencia rápida sobre la ubicación, la estructura, la misión y los datos.

CI

Contrainteligencia

3.4.5. Procedimiento de contraespionaje del equipo rojo

[3-92] A petición de un comandante de unidad o del comandante de la unidad superior de la que es orgánico, el personal de CI puede planear y ejecutar una simulación de recolección de información del enemigo. Tales simulaciones se conocen como *evaluaciones de seguridad de contraespionaje del equipo rojo*. Las evaluaciones de seguridad del equipo rojo identifican debilidades en la seguridad que podrían ser explotadas por el enemigo. Una vez completado este procedimiento, se emitirá una evaluación formal al comandante acerca de lo identificado, lo cual incluirá contramedidas y recomendaciones para superar, reducir o mitigar las vulnerabilidades. No hay una sola estructura o una sola composición para un equipo rojo. Las actividades del equipo rojo

se desarrollarán de acuerdo con el presente procedimiento, así:

- **Paso 1. Recolección de información previa:** dicha recolección establecerá un perfil previo de la unidad tomando en cuenta antecedentes, incidentes de CI, ambiente operacional y otra información de interés. Esta recolección se podrá hacer a través del comandante de la unidad apoyada, de los analistas o de las bases de datos de la disciplina de CI.
- **Paso 2. Monitoreo de actividades:** este monitoreo se realizará por medios humanos o técnicos dentro de la unidad apoyada, en lugares comúnmente frecuentados por personal que no tiene ningún grado de clasificación para el manejo de la información de interés para las propias tropas (basuras, casinos, tiendas, etc.), con el fin de obtener información que podría ser de interés para el equipo rojo (planes, bases de datos, datos biográficos, información de inteligencia, etc.). De esta forma se identifican vulnerabilidades y se permite la elaboración de las recomendaciones necesarias.
- **Paso 3. Sonsacamiento:** esta actividad es realizada por agentes en ambientes físicos o digitales para obtener información del personal objetivo, para determinar el nivel de concientización que dichos agentes poseen acerca de la información que se transmite voz a voz, y donde se podrían poner en riesgo planes u operaciones al comentarse información sensible en ambientes poco seguros.
- **Paso 4. Evaluaciones de contraespionaje:** actividades de simulación del equipo rojo para obtener el máximo posible de información en cuanto a las vulnerabilidades presentes en la unidad apoyada, y relacionadas con seguridad militar y seguridad de las operaciones, entre otras. Estas pruebas se podrán llevar a cabo en los ambientes físicos y digitales.
- **Paso 5. Análisis de la información:** los analistas de CI deberán analizar la información recolectada con el fin de clasificarla en una matriz de debilidades, oportunidades,

CI

Contrainteligencia

EEIPT CI	<p>Elementos esenciales de información de las propias tropas</p> <p>Contrainteligencia</p>
-------------------------------	--

fortalezas y amenazas, o cualquier otra matriz que el analista estime conveniente, a fin de refinar la información obtenida.

- **Paso 6. Difusión de la información:** esta debe ser recibida por el solicitante del procedimiento, y el comandante de la unidad que fue objeto de la actividad de CI —o quien haga sus veces—, y en ella se deben poner en conocimiento las vulnerabilidades, los EEIPT que deben protegerse y las contramedidas que deben tenerse en cuenta para solucionar las fallas de seguridad encontradas por el equipo rojo. La información sobre vulnerabilidades o fallas identificadas en la unidad debe generar una acción disciplinaria.

[3-93] Las actividades del equipo rojo pueden realizarse durante ejercicios tácticos, operaciones militares o juegos de guerra, siempre y cuando no afecten el normal desarrollo de estos. Todas las actividades del equipo rojo deben ser planeadas por el comandante de la unidad táctica y autorizadas por el comando de la Unidad Operativa Menor.

3.4.6. Procedimiento de gestión operacional

[3-94] La recolección de información está basada en la ejecución de tareas que buscan satisfacer los RICC o lograr identificar los EEIPT. Estas tareas se llevan a cabo mediante técnicas y procedimientos ejecutados por agentes de inteligencia y de CI. Tanto las técnicas y procedimientos, como los agentes, deben protegerse para el cumplimiento de los objetivos. Por tal motivo, se hace necesaria la implementación del procedimiento de gestión operacional.

[3-95] La gestión operacional es un procedimiento desarrollado por agentes de CI, la cual tiene como finalidad la implementación de fachadas e historias del personaje para proteger las actividades de inteligencia y de CI del conocimiento y las acciones de la amenaza buscando con ello la protección de los agentes, así como los medios de recolección de información empleados y las técnicas utilizadas.

[3-96] Este procedimiento se desarrolla con finalidades como:

- Fortalecer la seguridad de los agentes.
- Apoyar las técnicas de recolección de información realizadas de forma encubierta.
- Sustentar y soportar las historias del personaje.
- Garantizar el principio de la reserva legal de los recursos empleados para el desarrollo de las operaciones de inteligencia o de CI.
- Generar mecanismos administrativos seguros para minimizar los riesgos operacionales.
- Contribuir a la función de seguridad de personas.

CI

Contrainteligencia

[3-97] Este procedimiento consta de cinco pasos, los cuales se deben cumplir en el orden enunciado y serán ejecutados y desarrollados únicamente por agentes de CI:

- **Paso 1. Planeamiento:** el planeamiento se llevará a cabo de acuerdo con los requerimientos emitidos por las unidades solicitantes, o los planes establecidos por el comando superior. Este debe ser desarrollado por los agentes de CI que llevarán a cabo el procedimiento, en coordinación con el personal de la plana mayor y con el acompañamiento de un asesor jurídico. El comandante, el oficial de inteligencia y el oficial de operaciones deberán suministrar al personal designado la siguiente información:
 - Información previa de la amenaza.
 - Entendimiento de las variables de la misión.
 - Orden de operaciones.
 - Misión de trabajo (objetivo de la recolección de información, planeación de los requerimientos de información, técnicas para la recolección de información, instrucciones de coordinación).
 - Medidas de seguridad.
 - Planes de contingencia.

PEMSITIM	Política, económica, militar, social, información, tiempo, infraestructura y medio ambiente físico
METT-TC	Misión, enemigo, terreno y clima, tropas y apoyo disponible, tiempo disponible y consideraciones civiles

CI | Contrainteligencia

- **Paso 2. Recolección de información:** este paso se lleva a cabo para obtener información acerca de las variables operacionales (PEMSITIM) y servirá para establecer las variables de la misión (METT-TC) que permitan configurar el ambiente operacional.

De igual manera, la información recolectada se empleará como un criterio orientador para establecer cursos de acción previos al desarrollo de las operaciones de inteligencia y de CI.

Los agentes de CI adoptan y emplean las siguientes técnicas para la recolección de información, sin que sean las únicas:

- Entrevistas.
- Sonsacamiento.
- Estudio de los aspectos relevantes del ambiente operacional.
- Inteligencia de fuentes abiertas.

- **Paso 3. Análisis y evaluación:** Los agentes de CI, con base en la información recolectada durante el paso anterior, deberán hacer un análisis para determinar lo siguiente:

- Si la fachada o la historia del personaje se adapta al ambiente operacional: en este caso, se llevará a cabo una verificación con el fin de identificar los aspectos positivos y negativos, evaluar las observaciones y emitir recomendaciones.
- Si se requiere adecuar la fachada o la historia del personaje a las variables de la misión: en este caso, se deberán generar los cursos de acción para orientar la toma de decisiones del comandante de la unidad solicitante.

Las conclusiones del análisis efectuado se verán reflejadas en un informe de CI (ver el anexo A) del procedimiento operacional de CI.

- **Paso 4. Difusión de la información:** el informe generado en el paso anterior se deberá difundir al comandante de la unidad solicitante, teniendo en cuenta los criterios establecidos en el artículo 36 de la Ley 1621, referente a los receptores de información autorizados. La información contenida en este documento se constituirá para el comandante en un criterio orientador durante el proceso militar para la toma de decisiones (PMTD).

Una vez el comandante de la unidad solicitante haya recibido el informe, este deberá determinar cuál de los cursos de acción recomendados implementará, y deberá informar su decisión a la unidad de CI que desarrolló el procedimiento, a fin de darle continuidad a este.

- **Paso 5. Implementación:** de acuerdo con el curso de acción establecido por el comandante de la unidad solicitante, los agentes de CI desarrollarán el entrenamiento y la preparación del personal enfatizando y fortaleciendo temas relacionados con caracterización, lenguaje, expresión corporal y control del miedo, y los demás elementos necesarios para poder soportar una fachada y la historia del personaje en el AO.

En este paso también se entregarán los medios (técnicos, tecnológicos, de comunicación, de transporte o bienes inmuebles) necesarios para soportar la historia del personaje y mitigar el riesgo asociado con la seguridad de los agentes que se encuentran llevando a cabo la operación de inteligencia o de CI.

CI

Contrainteligencia

AO

Área de operaciones

3.5. LA CONTRAINTELIGENCIA EN LAS OPERACIONES MULTINACIONALES

AD

Acción decisiva

[3-98] Las operaciones multinacionales pueden incluir cualquier tipo de tarea dentro de las tareas de la AD, y deben hallarse enmarcadas dentro de una alianza, una coalición u operaciones de paz, así como alineados al marco legal colombiano, la normatividad internacional y las leyes de la nación anfitriona.

[3-99] Las alianzas son producto de acuerdos formales entre dos o más naciones, donde se establecen tiempo, motivos, objetivos y demás aspectos que los aliados crean necesarios. Estas alianzas son sinónimo de operaciones multinacionales.

[3-100] Una coalición militar depende de la alianza de las naciones, donde se especifican el tiempo y el propósito de esta. Por ejemplo, el despliegue de tropas colombianas a la península del Sinaí, con el fin de realizar operaciones de paz. Dicho despliegue incluye un esfuerzo conjunto para alcanzar el objetivo establecido, así como un cuartel compartido, donde se respete la jerarquía militar y se emplee el vocabulario doctrinal (VOCADOC), y donde se estén cumpliendo tareas alineadas doctrinalmente a las actividades desarrolladas con los otros ejércitos.

CI

Contrainteligencia

[3-101] Dentro de las operaciones multinacionales, la protección se establece como una responsabilidad del comandante, sin importar cuál sea su nacionalidad. Por tanto, dentro de sus actividades deberán incluirse las relacionadas con la disciplina de CI, para contrarrestar o neutralizar el ataque de las fuerzas enemigas a través de la negación de información a las redes de inteligencia de la amenaza.

[3-102] La CI se basa en el concepto de planeamiento centralizado y ejecución descentralizada; esto, debido a la sensibilidad y la criticidad de la información. La CI podrá apoyar limitadamente o con todos los medios disponibles de CI, dependiendo del tipo de alianza establecida, del ambiente operacional.

3.5.1. Actividades de constrainteligenzia en operaciones multinacionales

[3-103] Compartir información de CI es fundamental para el comandante y para la célula de protección. Los apoyos de CI a las operaciones multinacionales pueden incluir:

- Compartir técnicas para asegurar la información.
- Apoyar los acercamientos con organismos no gubernamentales.
- Realizar los procesos de inteligencia y gestión del riesgo en todos sus pasos basados en la capacidad de conocimiento de las fuerzas amigas.
- Desarrollar la arquitectura de inteligencia capaz de soportar la comunicación y la interoperabilidad.

CI

Contrainteligenzia

[3-104] La coordinación de estas actividades es fundamental para lograr una efectiva articulación de los esfuerzos de CI. En tal virtud, se deben aprovechar los lazos existentes para compartir información histórica que permita el conocimiento acerca del ambiente operacional y el empleo acertado de las actividades de la disciplina. Esta relación deberá incluir:

- Guías para proteger la información.
- Comprensión de la información obtenida acerca de las redes de inteligencia de la amenaza.
- Consideraciones especiales del área de operaciones (AO), tales como política, religión, cultura, idioma, entre otros que se consideren importantes.

[3-105] Dentro de la comprensión del ambiente operacional, existen condiciones cambiantes no solo dentro del área de operaciones multinacional, sino también, dentro de las naciones que apoyan la fuerza multinacional; debido a esto, se debe planear con cuidado el flujo de la información de CI, así como los mecanismos para su difusión.

[3-106] Cuando otra nación socia posea activos de CI, se deberá coordinar la recolección de información con el fin de aprovechar todos los medios disponibles y evitar la dualidad de esfuerzos.

[3-107] Las responsabilidades de las actividades de CI en operaciones multinacionales, se encontrarán en cabeza del oficial asignado para tal fin, quien será el directo encargado de todas las actividades de CI desarrolladas durante las operaciones multinacionales.

[3-108] Independientemente de las alianzas establecidas, del ambiente operacional o de la nación apoyada, los agentes deberán regirse, principalmente, por las leyes y las normas vigentes en Colombia y por las que regulan a la nación anfitriona. Asimismo, el comandante de CI deberá velar por el cumplimiento de dichas leyes y normas.

[3-109] Muchas naciones aliadas no manejan la misma organización de CI, o bien desarrollan diferentes procedimientos o técnicas para la recolección de información. Por tal motivo, se hace necesario en el predespliegue la coordinación de estas actividades, al igual que la ejecución mancomunada durante toda la operación.

CI

Contrainteligencia

3.5.2. Organización de contrainteligencia en operaciones multinacionales

[3-110] La CI se desplegará en operaciones multinacionales u operaciones de paz y actuará dentro de la organización de inteligencia del estado mayor de la fuerza multinacional.

[3-111] Las siguientes son algunas consideraciones que deberán tener en cuenta las unidades de CI en las operaciones multinacionales:

- La CI mantendrá el mando operacional de todos los activos de CI puestos a disposición de las operaciones multinacionales.

- El comandante de CI o el oficial coordinador, deberá cumplir sus funciones dentro de la organización del estado mayor.
- Si se requiere el apoyo de agentes de CI en cubierta, se deberán analizar por anticipado el ambiente operacional, las leyes locales y la normatividad colombiana.
- El comandante de CI determinará con qué activos de CI apoyará la fuerza multinacional.
- Los agentes de CI deberán tener un manejo del idioma acorde con el utilizado por la fuerza multinacional; como mínimo, nivel B2.

CI | Contrainteligencia

RICC | Requerimientos de información crítica del comandante

[3-112] De igual forma, el personal de agentes que efectúe la operación deberá contar con un material específico, que les permita responder los RICC, al asumirse estos como indispensables para lograr el máximo de eficiencia en las actividades de CI. Dicho material incluye:

- Instalaciones fijas o móviles que cuenten con la seguridad suficiente para integrar el trabajo de CI.
- Sistemas informáticos que garanticen el flujo de información.
- Computadores portátiles y fijos.
- Discos duros.
- Sistemas biométricos
- Cámaras de video y fotográficas, así como minicámaras.
- Sistemas de explotación de documentos y programas de traducción.
- Sistemas de comunicación eficientes (medios de comunicación, como celulares, radios, etc.).

[3-113] Del mismo modo, los agentes de CI deberán contar con una partida de gastos reservados, para su uso en operaciones

de CI, para el pago de información o para cualquier actividad derivada de las actividades propias de la disciplina.

3.5.3. Recolección de información y reportes en las operaciones multinacionales

MRI Medios de recolección de información	<p>[3-114] La participación en operaciones multinacionales ofrece una oportunidad única para recolectar información a través de los MRI de la coalición y de los servicios de inteligencia existentes. Esta unión de esfuerzos de inteligencia contribuye significativamente a la recolección de información de CI de una manera más efectiva que la recolección efectuada por una sola nación.</p> <p>[3-115] El manejo de los requerimientos de información es responsabilidad del comandante de CI.</p> <p>[3-116] Los agentes de CI deberán disponer de computadores seguros y aparatos electrónicos que faciliten la comunicación con el oficial de CI, al igual que con el procesamiento y el resguardo de la información adecuados.</p>
CI Contrainteligencia	<p>[3-117] Los reportes deberán ser transmitidos por canales de comunicación seguros. Los reportes que indiquen una amenaza inminente para las operaciones militares o el MTM deberán ser difundidos no solo al oficial de CI, sino también, al comandante militar, y bajo el cumplimiento estricto de las medidas establecidas por OPSEC.</p>
MTM Mando tipo misión	
OPSEC Seguridad de las operaciones	

3.5.4. Análisis de contrainteligencia en las operaciones multinacionales

[3-118] Las relaciones y las coordinaciones entre la parte militar y civil permiten el empleo de mayor cantidad de fuentes de información. En algunos casos, una nación puede tener una mejor base de datos que otra que cuente con información de interés para la nación solicitante.

[3-119] La precisión de los análisis de información de CI, dependerá directamente de la información y de los recursos puestos a disposición por las agencias asociadas que participan en las operaciones multinacionales.

[3-120] La difusión de información de CI deberá ser únicamente bajo los canales de comunicación autorizados, ya sea al comandante militar o al oficial de CI.

3.5.4.1. Empleo de herramientas analíticas de contrainteligencia en operaciones multinacionales

CI

Contrainteligencia

[3-121] El empleo de herramientas analíticas permite a los analistas y a los usuarios de la información el planeamiento, el análisis y la focalización de los requerimientos de información. Los agentes de CI ubicados en el área proveen insumos de información a los analistas acerca de personas, organizaciones, instalaciones y otros elementos importantes del AO.

AO

Área de operaciones

[3-122] Estas herramientas facilitan el procesamiento de información con matrices de análisis basadas, a su vez, en los eventos de tiempo y en la relación de contacto entre personas de interés, diagramas y productos de visualización. Estas herramientas permiten una mejor visualización del ambiente operacional para desarrollar anticipaciones de la acción de la amenaza identificando brechas de información y respaldando los planes del Ejército. Asimismo, permite:

- Hacer seguimiento a los reportes de CI.
- Recuperar datos.
- Automatizar y visualizar matrices.
- Compartir productos de los análisis de CI con el personal de la disciplina desplegada en el AO en tiempo real.
- Aplicar variedad de tecnologías basadas en las diferentes técnicas desarrolladas por cada nación.
- Visualizar en tiempo real las operaciones de CI.

- Compartir recursos, modelos, mapas, calcos y herramientas a través de programas comunes.
- Descubrir indicadores, patrones y relaciones de la amenaza que puedan llevar a anticipar acciones de esta.

3.6. APOYOS DE CONTRAINTELIGENCIA

[3-123] La contrainteligencia apoya a las funciones de conducción de la guerra, las actividades de la acción unificada, la acción decisiva, así como planes o tareas del Ejército. Dichos apoyos buscan asesorar, contribuir, intervenir o hacer parte de estas, de forma activa y funcional.

3.6.1. Apoyo al proceso de selección y priorización de blancos

[3-124] El apoyo de la CI consiste en interrumpir, retrasar o limitar la interferencia de la amenaza con los cursos de acción propios; esto requiere una interacción coordinada entre el personal de operaciones, inteligencia y CI. Se deberá hacer una evaluación antes de comprometer el poder de combate destinado a neutralizar objetivos prioritarios, y la corroboración de la información debe ser mancomunada con la integración de otras disciplinas de la FCG Inteligencia, esto ayudará a validar el objetivo, y así evitar esfuerzos innecesarios y desgaste de recursos humanos y técnicos.

CI	Contrainteligencia
FCG	Función de conducción de la guerra

3.6.2. Apoyo mediante la realización de estudios y recomendaciones de seguridad

[3-125] Los agentes de CI llevan a cabo estudios, inspecciones o cualquier otro tipo de actividad para generar recomendaciones de seguridad en todos los niveles, a fin de mejorar la seguridad de las organizaciones o las unidades apoyadas. Estas actividades ayudan a los comandantes a desarrollar, mantener o mejorar las condiciones de seguridad. Dicho apoyo se

enfoca en ayudar a identificar y neutralizar las amenazas a la seguridad que intentan obtener información, y con ello se busca proporcionar información sobre la amenaza e identificar vulnerabilidades específicas que requieren tratamiento para su mitigación. Esta actividad puede incluir, entre otros:

- Estudios de seguridad de rutas.
- Inspecciones de seguridad (físicas y técnicas).
- Capacitaciones sobre seguridad.
- Evaluaciones técnicas de seguridad de la información.
- Evaluaciones de seguridad.

CI

Contrainteligencia

3.6.3. Apoyo a las actividades contra el narcotráfico

[3-126] La CI desarrolla tareas y actividades para apoyar a otras unidades o agencias responsables de identificar, detectar e interrumpir las acciones llevadas a cabo por entidades u organizaciones de tráfico ilícito de drogas, incluyendo su estructura (personal, material, infraestructura y sistemas de distribución). Asimismo, identifica, detecta y neutraliza a personal del Ejército o de los asociados de la AU que tengan vínculos con grupos al margen de la ley o a quienes reciban cualquier tipo de beneficio por actividades de narcotráfico. Si es necesario, se nombrarán analistas de CI en apoyo de las unidades que se encargan de neutralizar los grupos al margen de la ley dedicados a esta actividad.

AU

Acción unificada

3.6.4. Apoyo a las actividades de guerra electrónica

[3-127] La guerra electrónica (EW, por su sigla en inglés) es la acción militar que implica el uso de energía electromagnética y dirigida a controlar el espectro electromagnético o para atacar al enemigo (MFRE 3-0).

[3-128] La CI aporta a las actividades de guerra electrónica (EW) a través de:

EW	Guerra electrónica
EMS	Espectro electromagnético
CI	Contrainteligencia

- Proporcionar apoyo a la técnica de protección electrónica de la disciplina de EW mediante el diseño de protocolos dirigidos a incrementar la seguridad electrónica, a fin de negar información de valor acerca de las actividades de EW mitigando las emisiones de EMS y aumentando la protección de red, y logrando, a su vez, potenciar la degradación de la capacidad de la amenaza de recolectar información.
- Proveer protocolos de seguridad de personal, a fin de protegerlo de las manipulaciones de la amenaza que puedan causar la degradación o el daño de las capacidades propias.
- Suministrar guías y directrices para mejorar la seguridad de las instalaciones y los equipos de EW para protegerlos de la acción de elementos adversarios o de enemigos que puedan afectar las capacidades o las tecnologías propias.
- Apoyar a la comprensión del ambiente operacional de guerra electrónica a través del aporte de apreciaciones de CI que faciliten el entendimiento de las capacidades de la inteligencia enemiga o adversaria, y, de esta forma, prevenir futuras acciones que impidan o retarden las acciones de EW propias.

3.6.5. Apoyo a la seguridad de las operaciones

[3-129] La *seguridad de las operaciones* (OPSEC, por su sigla en inglés) es el proceso de identificación, análisis y protección de la información crítica durante el proceso de operaciones (MFRE 3-37). Es una tarea que dificulta el uso de sus propios sistemas y procesos de información por parte del adversario, proporcionando el apoyo necesario a todas las capacidades de las propias tropas para el desarrollo de operaciones de información.

[3-130] Este procedimiento consta de cinco (5) pasos continuos, que se aplican de una manera lógica para identificar y

mitigar los indicadores de intenciones, capacidades, operaciones y actividades del enemigo.

- **Paso 1.** Identificar información sensible/crítica.
- **Paso 2.** Analizar las amenazas/adversarios.
- **Paso 3.** Analizar vulnerabilidades.
- **Paso 4.** Evaluar riesgos.
- **Paso 5.** Aplicar contramedidas

CI | Contrainteligencia

[3-131] La CI apoya a la OPSEC así:

- Identifica la inteligencia de la amenaza.
- Conoce los métodos de recolección de la amenaza.
- Analiza las capacidades de explotación de la amenaza.
- Niega a la amenaza la recolección de información necesaria para evaluar las intenciones de las propias tropas.
- Aplica contramedidas para mitigar la recolección de información de la amenaza.

OPSEC | Seguridad de las operaciones

[3-132] OPSEC contribuye a la planeación, la evaluación y la ejecución de operaciones de la unidad apoyada por la CI en torno a la protección de información crítica, con el fin de liderar las actividades pertinentes por parte de la Fuerza, y que conciernen a la preservación del secreto como elemento esencial para el desarrollo de todas las operaciones militares.

3.6.6. Apoyo a la contrapropaganda

[3-133] La contrapropaganda es cualquier forma de comunicación para apoyar objetivos nacionales diseñados con el objeto de influir en las opiniones, las emociones, las actitudes o el comportamiento de cualquier grupo para beneficiar al interesado, ya sea directa o indirectamente. Normalmente, está dirigido por agencias de Colombia, asociadas de la AU, y se

AU | Acción unificada

AO Área de operaciones

encuentran destinadas a audiencias clave en el AO. Las actividades de propaganda desarrolladas por la amenaza están diseñadas deliberadamente para atacar la voluntad de las naciones de resistir, y la de los soldados, de luchar. Buscan mezclar la verdad y la mentira de una manera que las audiencias no puedan determinar en qué momento se sesga la realidad y se produce la desinformación.

[3-134] La contrapropaganda está estructurada para detectar y contrarrestar los intentos del adversario de transmitir mensajes específicamente diseñados para la audiencia colombiana, y encaminados a influir en sus emociones, sus motivaciones, sus razonamientos y sus objetivos, y, en última instancia, en el comportamiento del gobierno, de las organizaciones, de los grupos y de los individuos. La contrapropaganda identifica la propaganda del adversario y contribuye a generar una conciencia situacional que sirva para exponer los intentos del adversario de influir en las poblaciones amigas y en el personal de las fuerzas militares.

CI Contrainteligencia

[3-135] La CI apoya los esfuerzos de la contrapropaganda proporcionando información acerca de las actividades de propaganda adversarias. Es posible que la CI conozca el inminente mensaje de propaganda del adversario antes de que este divulgue la información. Eso proporciona la oportunidad y la ventaja militar para adelantarse a la emisión del mensaje de la amenaza y contrarrestarlo mediante la producción y la emisión de mensajes propios. La CI identifica la propaganda del adversario a través de las actividades, las funciones, las operaciones y las competencias distintivas de esta disciplina.

3.6.7. Apoyo a la contrafakección

[3-136] La *decepción*, entendida como el conjunto de medidas dirigidas a inducir al error al enemigo por medio de la manipulación, la deformación o la falsificación de evidencias para hacerle actuar de forma perjudicial a sus intereses (MFRE 3-37), y ejecutada en contra de la Fuerza, requerirá la aplicación de actividades de CI destinadas a apoyar la contrafakección negando, contrarrestando y neutralizando los

efectos de la actividad enemiga y obteniendo una ventaja de la operación de engaño de un adversario. Saber qué métodos de engaño ha usado un adversario en el pasado es importante. También lo es considerar los indicadores, y no descartarlos tan solo porque entren en conflicto con ideas preconcebidas, pues esto permitiría que el engaño hecho por un adversario tenga éxito.

[3-137] El análisis de CI proporciona conciencia de la postura o la intención de un adversario e identifica el intento del adversario de engañar a las fuerzas amigas. La prioridad de recolección de inteligencia de un adversario puede proporcionar indicadores acerca de sus requisitos de recolección reales y de su propio plan de engaño. Es necesario no solo descubrir el plan de engaño del adversario, sino, a su vez, impedir que este conozca lo que de él se ha descubierto.

CI

Contrainteligencia

[3-138] La CI puede identificar las actividades realizadas por la inteligencia de la amenaza que se desarrollen en contra de la Fuerza intentando descubrir lo que ya se sabe sobre su plan de engaño.

3.6.8. Apoyo contra el tráfico de armas de fuego, municiones y explosivos de uso privativo de las Fuerzas Militares

[3-139] Este apoyo será llevado a cabo mediante el desarrollo de la técnica de trazabilidad y rastreo, que comprende un conjunto de actividades determinadas, ejecutadas por la disciplina de CI para establecer el origen, la asignación, la distribución y el destino final de las armas de fuego, las municiones y los explosivos de uso privativo de las Fuerzas Militares que se hallen en custodia en las unidades militares, así como el incautado o recuperado en el desarrollo de operaciones.

[3-140] El objetivo de esta técnica es proporcionar un entendimiento de las acciones de la amenaza que permita orientar los esfuerzos destinados a la preservación del material de activos fijos (armas de fuego) y material de consumo (granadas y municiones), y que conlleve prevenir, detectar y

contrarrestar el tráfico de material de guerra efectuado por redes de inteligencia extranjera, organizaciones terroristas u otros enemigos o adversarios, que con esta actividad buscan obstaculizar o disminuir la eficiencia del actuar militar.

CI | Contrainteligencia

[3-141] Esta actividad de CI empleará el sistema de aplicación de procesamiento de productos y datos (SAP), el cual es utilizado para efectuar la trazabilidad y el rastreo del material de guerra que es incautado en el desarrollo de operaciones, y sirve, así como medio orientador para la recolección de información sobre la posible fuga o el tráfico de dicho material, que ingresa al territorio colombiano por medio del crimen trasnacional organizado. De la misma forma, el empleo de este sistema permite generar cursos de acción, a fin de contrarrestar la fuga de material en las unidades militares.



ADN BICENTENARIO

INCURSIÓN DE GRUPOS DE CRIMEN ORGANIZADO TRANSNACIONAL EN TERRITORIO COLOMBIANO

A mediados de 2016, la CI del Ejército, mediante el empleo de agentes encubiertos, obtiene información acerca de la incursión en territorio colombiano de un grupo de crimen organizado transnacional, conformado por personas de diferentes nacionalidades. La información recolectada indicaba que este grupo se encontraba fraccionado en varias células ubicadas en zonas fronterizas, donde estarían promoviendo el tráfico de personas provenientes de Cuba y de Venezuela.

La información inicial permitió la configuración de dos operaciones de CI que fueron ejecutadas simultáneamente. La operación de contraespionaje estaba dirigida al tráfico de información que estaba llevando a cabo el mencionado grupo a través de mujeres de nacionalidad venezolana que eran empleadas como trabajadoras sexuales y, a su vez, utilizadas como informantes. La segunda, que fue catalogada como una operación de contraterrorismo, se direccionó a la identificación de los vínculos que tenía dicho grupo con otras organizaciones nacionales al margen de la ley, con las cuales coordinaban actividades de narcotráfico y negociaban el ingreso de armamento ilegal al territorio colombiano utilizando rutas clandestinas desde Venezuela y Ecuador.

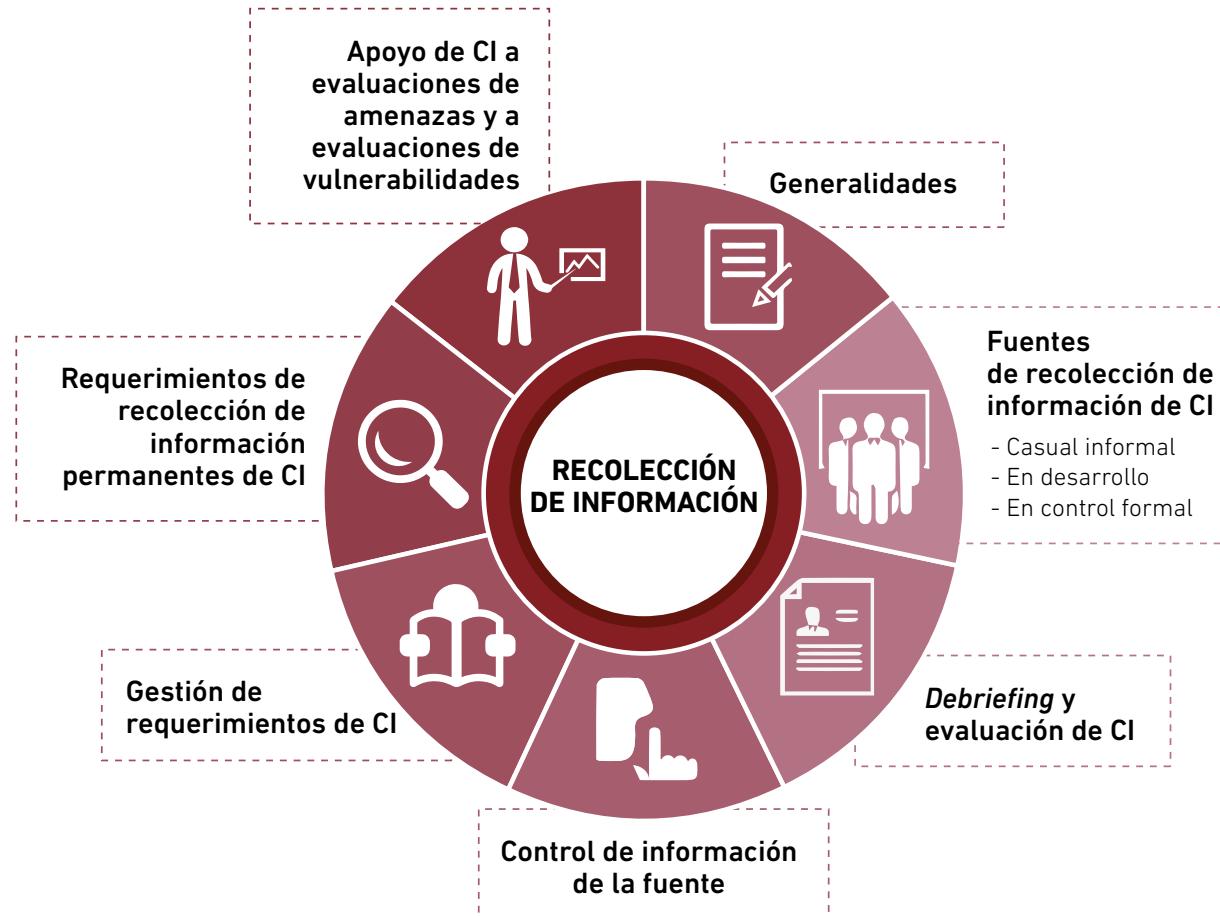
El resultado de las dos operaciones se materializó en la captura de 49 extranjeros y una persona que poseía doble nacionalidad, y los cuales fueron deportados a sus respectivos países de origen.

CAPÍTULO 4

RECOLECCIÓN DE INFORMACIÓN

"El campo de batalla es una escena de caos constante. El ganador será el que lo controla, tanto el propio como el de los enemigos".

Napoleón Bonaparte



[4-1] La unidad operativa mayor de CI proporciona apoyo a las unidades operativas mayores, menores y tácticas en materia de recolección de información. La recolección de información de CI es la obtención sistemática de información de la inteligencia extranjera, servicios de seguridad, organizaciones terroristas, agentes locales y otras amenazas.

4.1. GENERALIDADES

FCG	Función de conducción de la guerra
RICC	Requerimientos de información crítica del comandante
CI	Contrainteligencia
RIPT	Requerimiento de información de las propias tropas
EEIPT	Elementos esenciales de información de las propias tropas

[4-2] La inteligencia y la CI hacen uso de todas las disciplinas de la FCG Inteligencia para recolectar información; sin embargo, la diferencia primordial entre las dos actividades se encuentra en el objetivo de cada una, como se muestra a continuación:

- **La inteligencia conoce la información del adversario:** la recolección de información de inteligencia está enfocada en responder satisfactoriamente los RICC y en identificar planes y capacidades de la amenaza, así como el terreno, el clima y las consideraciones civiles, con el fin de conocer el ambiente operacional.
- **La CI evita que la amenaza conozca la información propia:** la recolección de información de CI está enfocada en responder los RIPT (EEIPT) y los RICC (concernientes a CI), así como en conocer los métodos e intenciones de las redes de inteligencia u otras amenazas, con el fin de proteger la Fuerza y negar información al adversario.

| Tabla 4-1 | Diferenciación entre inteligencia y CI

	INTELIGENCIA	CONRAINTELIGENCIA
RESPONDE	RICC	RIPT (EEIPT) - RICC (concernientes a la disciplina de CI)
RECOLECTA	Planes Capacidades	Métodos Intenciones
BUSCA	El conocimiento del adversario	Afectar el conocimiento del adversario acerca de la Fuerza
PROpósito	Atacar la amenaza	Proteger la Fuerza
OBJETIVO	Acceder a la información de la amenaza	Negar el acceso a información

[4-3] La recolección de CI se enfoca principalmente en las actividades de inteligencia de la amenaza, y se centra en la identificación y detección de inteligencia extranjera y servicios de seguridad (FISS, por su sigla en inglés), organizaciones terroristas (OT), agentes locales y otras amenazas, ya sea para prevenir, disuadir, interrumpir, explotar, contrarrestar o neutralizar sus acciones. El objetivo de la recolección de información de CI es poder:

- Afectar el conocimiento de los planes, las intenciones y las capacidades de la inteligencia del adversario.
- Negar la recolección de información para atacar a las fuerzas propias.
- Negar, mitigar o interrumpir las capacidades de FISS, OT, agentes locales y de otras amenazas.
- Identificar al personal de la Fuerza que se encuentre en riesgo o haya sido subvertido por parte de la amenaza, y que represente un riesgo para la seguridad.

CI | Contrainteligencia

FISS | Inteligencia extranjera y servicios de seguridad

OT | Organizaciones terroristas

4.2. FUENTES PARA LA RECOLECCIÓN DE INFORMACIÓN DE CONTRAINTELIGENCIA

[4-4] Esta tarea se ejecuta a través de un plan de recolección de CI que abarca tres tipos de fuentes de información. Cada una de ellas es distinta de las demás en cuanto a la sensibilidad, el objetivo al que se dirige y el proceso de aprobación requerido para la ejecución de la actividad de recolección necesaria.

AU	Acción unificada	[4-5] Las actividades de recolección de información de CI apoyan a los asociados de la AU, así como a las unidades operativas mayores, menores o tácticas; sin embargo, los requerimientos de CI se harán a través del Comando de Apoyo de Combate de Contrainteligencia Militar (CACIM).
CI	Contrainteligencia	[4-6] Existen tres tipos de fuentes, que se establecen de acuerdo con el control que ejerce un agente sobre ellas.

| Tabla 4-2 | Tipos de fuentes de información

Casual informal	<ul style="list-style-type: none"> Fuentes esporádicas. Brindan información acerca del ambiente operacional, la cual debe ser corroborada por otras fuentes. No se les asigna tareas de recolección de información. Registro en unidad táctica.
En desarrollo	<ul style="list-style-type: none"> Fuentes continuas. Brinda información más detallada y completa. Requiere evaluación constante de la fuente. Registro en unidad operativa menor.
En control formal	<ul style="list-style-type: none"> Las fuentes cuentan con examen psicofisiológico de polígrafo. Su información es altamente creíble y poseen historial de informes de CI. Se les asignan tareas de recolección de información. Registro en unidad operativa mayor.

4.2.1. Casual informal

[4-7] Fuentes únicas esporádicas o contactos casuales que pueden proporcionar datos del ambiente operacional, así como riesgos y amenazas presentes en este. El agente tiene

un control mínimo sobre la fuente; por tal motivo, la información tiene que ser evaluada y confrontada con los MRI disponibles para lograr emitir un criterio acerca de la credibilidad de la información y la confiabilidad de la fuente.

MRI | Medios de recolección de información

[4-8] Este tipo de fuentes normalmente suministra información a los analistas operacionales o a los enlaces en las unidades militares o en las entidades gubernamentales.

[4-9] A las fuentes que proveen este tipo de información no se les asignan tareas de recolección; esto, en razón de su falta de preparación para el desarrollo de actividades de ISR (por su sigla en inglés) que podrían vulnerar su propia seguridad y elevar el riesgo operacional de la misión al haber vacíos de información acerca de la procedencia y la intención de la fuente.

[4-10] Esta fuente será registrada por la unidad táctica como una referencia, que permita establecer un historial acerca de la información obtenida.

4.2.2. En desarrollo

[4-11] Fuentes que han sido contactadas o trabajadas de forma rutinaria y pueden proporcionar información más detallada y completa que una fuente informal. Este tipo de fuentes ha suministrado información de valor relacionada con los intereses de Colombia o de la Fuerza.

[4-12] Se requiere una evaluación constante de la información suministrada por medio del cruce de esta con más fuentes de inteligencia.

[4-13] A estas fuentes se les podrán practicar pruebas técnicas psicofisiológicas de veracidad, para evaluar su credibilidad y confiabilidad de forma periódica y con el previo consentimiento informado de la fuente, para verificar el manejo de información y los propósitos que tiene al estar desarrollando las actividades.

[4-14] Esta fuente será registrada por la unidad operativa menor, como una referencia acerca del origen de la información,

estableciendo la confiabilidad de la fuente, y si se encuentra activa o en desarrollo.

4.2.3. En control formal

[4-15] Son fuentes que cuentan con un historial de informes dentro de la labor de CI. A estas fuentes se las considera confiables, debido a que han sido evaluadas o examinadas por agentes de CI. Las fuentes controladas han acordado voluntariamente reunirse y cooperar con agentes, a fin de proporcionar información.

[4-16] Se le puede asignar tareas de recolección de información enfocadas en información específica extraída de solicitudes de información (SI) o del desarrollo de las operaciones; esto, con el fin de entregar al agente información en la cual basar sus asociaciones laborales, sociales o geográficas en cumplimiento de la misión, de modo que esto le permita efectuar eficazmente las tareas asignadas. Las reuniones entre el agente y la fuente controlada serán las mínimas necesarias para garantizar la seguridad de las partes y se efectuarán extremando las medidas de seguridad en cada una de ellas.

CI

Contrainteligencia

[4-17] Esta fuente será registrada por la unidad operativa mayor y se le asignará código operacional.

4.3. DEBRIEFING Y EVALUACIÓN

[4-18] Gran cantidad de la información obtenida por los agentes es recolectada durante el desarrollo de actividades de la disciplina desarrolladas de forma abierta, y dentro de las cuales se pueden incluir el *debriefing* y las evaluaciones de CI.

4.3.1. *Debriefing* de contrainteligencia

[4-19] *Debriefing* es definido como la **actividad que busca obtener información a través de preguntas sistemáticas respecto a un tema particular**.

[4-20] La CI deberá efectuar un *debriefing* al personal de la fuerza o de los asociados de la AU que, dada su actividad sensible fuera del país (Colombia), pudieron haber tenido contacto con agencias de inteligencia enemiga. Este personal incluye a las unidades de combate que se encuentren efectuando tareas dentro del marco de la AU y a aquel personal que debido a su cargo o sus funciones haya tenido contacto con personal enemigo o adversario y por ende requiera ser sometido a actividades de debriefing o evaluación de CI.

[4-21] Como resultado del *debriefing*, se debe generar un informe de CI donde se plasmen los aspectos de interés que podrían apoyar las operaciones de CI o dar inicio a una averiguación o una operación.

AU | Acción unificada

CI | Contrainteligencia

4.3.1.1. *Debriefing* de ausentes de categoría especial

[4-22] Ausentes de categoría especial son:

- Personas que se encuentran ausentes de sus cargos, sus funciones o sus áreas de responsabilidad sin la debida autorización o el permiso previo.
- Personas que viajan sin autorización a un país extranjero.
- Personas de quienes se corrobore la intención de recolectar información de la fuerza o de los asociados de la AU.

[4-23] Aunque los ausentes de categoría especial no actúen de forma directa en la vulneración de la seguridad nacional o en un incidente de CI, es la naturaleza de su ausencia y por las circunstancias relativas a su contacto con la inteligencia del adversario, la razón por la cual se les debe indagar, para identificar y obtener la mayor cantidad de información de interés para la CI. Los informes se centrarán, como mínimo, en los siguientes aspectos:

- Circunstancias que rodearon la ausencia (motivación y destino planificado).

- Personas u organizaciones con las que tomó contacto o a quienes suministró apoyo.
- Visitas a cualquier organización diplomática o gubernamental extranjera durante el espacio de ausencia.
- Viaje hacia o a través de un país durante la ausencia, y todas las actividades que ocurrieron durante dicho viaje.
- Contacto con representantes o personas de un gobierno extranjero o con una OT.
- Tipo de información, clasificada o no, a la que tuvo acceso y proporcionó a la persona o la organización no autorizada.

OT | Organizaciones terroristas

CI | Contrainteligencia

4.3.1.2. *Debriefing a los desertores*

[4-24] La CI llevará a cabo actividades de CI con el personal de desertores, a fin de obtener información acerca de las actividades realizadas durante el tiempo de ausencia del servicio, so pena de las acciones legales a que haya lugar. Luego emitirá los informes pertinentes, independientemente de si tuvieron acceso o no a información clasificada. Los informes de desertores se centrarán, como mínimo, en:

- Circunstancias, motivación en torno a la deserción y su destino planificado.
- Personas u organizaciones con las que el desertor tomó contacto o las que le brindaron apoyo.
- Descripciones completas e información que permita la identificación de personal de inteligencia extranjera, entrevistadores u otros funcionarios con quienes el desertor tuvo contacto.
- Fuente de financiación durante el periodo de deserción.
- Determinar si los desertores usaron alias o identificaciones falsas o si ocultaron sus identidades; en caso de ser así, ¿a través de quién y cómo se obtuvo la documentación?

- Identificación de equipos de cómputo, medios de comunicación, *hardware* o cualquier documento clasificado que el desertor haya tenido en su poder y haya entregado a personal no autorizado.
- Detalles del viaje, incluido el modo de transporte, el itinerario, las ciudades o países a los que se haya viajado, los medios y la documentación empleada para el cruce de fronteras internacionales.
- Detalles de todas las conversaciones, los interrogatorios o las entrevistas en que el desertor participó: identidad y descripciones físicas de las partes (interrogadores o entrevistadores), métodos empleados, cooperación del desertor, respuestas del interrogador al rechazo del desertor a cooperar o incapacidad para responder una pregunta.
- Naturaleza y alcance de cualquier propaganda y exposición de medios dada al desertor.
- Respuesta del gobierno extranjero a la presencia de desertores en otro país.
- Detalles completos acerca de cualquier contacto con otros desertores colombianos, incluyendo datos de identificación como nombres, descripciones físicas, unidades de asignación, nivel de acceso a información clasificada, antecedentes familiares, lugares de residencia, última ubicación conocida, cooperación conocida o sospechada con inteligencia extranjera u otros funcionarios, razones para la deserción y actitud actual respecto a su deserción.

4.3.1.3. *Debriefing* personal liberado

[4-25] Los agentes realizan un *debriefing* a personal militar, civil y aquel contratado por el Ejército, que haya sido privado de la libertad por fuerzas extranjeras, gobiernos extranjeros, grupos terroristas o servicios de inteligencia en razón de su función o su cargo. Esto se materializará en un informe, que, como mínimo, se enfocará en:

OT

Organizaciones
terroristas

- Circunstancias de la captura o la detención.
- Descripciones físicas e información completa de los miembros de inteligencia extranjera, OT o servicios de seguridad.
- Ubicación de puestos de mando, instalaciones militares, casas de seguridad, centros de detención y otros.
- Descripción de las técnicas de interrogatorio, preguntas formuladas e información entregada.
- Condiciones o exigencias para su liberación.
- Identidad y ubicación de los prisioneros de guerra, los detenidos y los desertores; tratamiento recibido y condiciones físicas y mentales.
- Descripción de cualquier información reservada o clasificada, o material y equipo empleado por el enemigo.

4.3.1.4 Debriefing a agentes de inteligencia o contrainteligencia

CI

Contrainteligencia

[4-26] Este tipo de actividad, generalmente, se lleva a cabo debido a que los agentes de inteligencia y de CI se encuentran en constante contacto con el adversario, pues su actividad está basada en la administración de fuentes y en la recolección de información dentro de la organización del adversario. Durante este proceso pueden ser objeto de la acción de la amenaza, y, por tal motivo, serán indagados a su regreso, para obtener cualquier información de inteligencia o de CI de interés, la cual deberá ser plasmada en un informe, siempre y cuando la información obtenida aporte insumos para la toma de decisiones.

4.3.2 Evaluación de personal para obtención de información de contrainteligencia

[4-27] Consiste en un proceso sistemático donde a una persona específica o a una audiencia objetivo se les aplica una variedad de técnicas o procedimientos, que tienen como propósito la obtención de información. Para tal fin, se podrán aplicar las siguientes actividades, sin ser las únicas:

- Entrevistas de CI.
- Exámenes psicofisiológicos de polígrafo.
- Estudio de credibilidad y confiabilidad.
- Utilización del **sonsacamiento**, definido como **técnica discreta de entrevista, que no le permite al entrevistado conocer la intención específica del agente**.

CI

Contrainteligencia

[4-28] Cada una de estas actividades se puede usar o combinar dependiendo de la situación. Por ejemplo, durante una entrevista, si el entrevistado proporcionara una ventaja fuera del alcance de la lista de preguntas, pero de interés para la CI, el agente podrá hacer la transición a otro tipo de técnica, con el fin de explotar la situación y obtener información adicional.

[4-29] La CI podrá establecer la evaluación de personal para obtención de información de CI como una actividad de alta prioridad, que de acuerdo con la información recolectada generará informes de CI significativos para el PMTD, y así permite identificar amenazas y riesgos, lo cual lleva a la realización de averiguaciones u operaciones de CI.

PMTD

Proceso militar
para la toma de
decisiones

[4-30] Durante la evaluación de personal de CI, los entrevistados son analizados, con el propósito de determinar posibles indicadores o patrones de recolección de información por parte del adversario.

[4-31] La evaluación de personal de CI requiere recursos y apoyo de los comandantes para facilitar el desarrollo de sus actividades. El equipo, las instalaciones y el personal son

necesarios para la realización de estas evaluaciones, las cuales deberán identificarse en el planeamiento. Por ejemplo:

[4-32] El equipo incluye los sistemas biométricos utilizados para identificar y rastrear antecedentes del examinado. Esto permite a los agentes determinar a las personas asociadas a eventos o informes de inteligencia y CI que han sido previamente seleccionadas. Dentro del equipo también se pueden considerar grabadoras de voz, cámaras u otros elementos que coadyuven a la recolección de información.

[4-33] Las instalaciones incluyen espacio que ofrece privacidad y seguridad durante el proceso. En el desarrollo de las evaluaciones de CI no se debe permitir que el personal que está esperando a ser evaluado tenga la oportunidad de escuchar o conocer evaluaciones previas de otro personal. La falta de privacidad facilita que un posible recolector de información de la amenaza tenga la oportunidad de enterarse de las entrevistas en curso y formular respuestas con base en información previamente elaborada, y así evadir a los agentes de CI. Se deben hacer controles de seguridad previos a la evaluación empleando procedimientos de seguridad física y seguridad de información, como las contramedidas electrónicas y cualquier otro que sea necesario para mantener el curso normal de la evaluación. Para ello, será esencial la coordinación con personal de la unidad, que haga los requerimientos pertinentes a las unidades de seguridad militar y de policía militar.

CI

Contrainteligencia

[4-34] En caso de ser necesario el uso de intérpretes, estos deben ser seleccionados bajo los estándares de credibilidad y confiabilidad del Ejército Nacional (seguridad de personas). En el planeamiento se debe tener en cuenta qué idioma y/o dialectos requiere, de intérpretes, así como la cantidad de personal necesario para dar cumplimiento a la misión.

4.4. CONTROL DE INFORMACIÓN DE LA FUENTE

[4-35] Todas las actividades de recolección requieren mantener registros de las fuentes de CI. Esto es cierto tanto para los

contactos de enlace como para las fuentes formales o informales. Los datos sobre las fuentes de CI se ingresarán en los registros de fuentes y agencias.

[4-36] El control de la información inicial no impedirá el paso de este tipo de información de un escalón a otro para las aprobaciones necesarias. Al manejar la información inicial, se debe seguir estrictamente el lema de "necesidad de saber". El número de personas que conocen la información inicial y subsiguiente debe mantenerse al mínimo y tener trazabilidad documental, aplicando el principio de compartimentación.

4.5. GESTIÓN DE REQUERIMIENTOS DE CONTRAINTELIGENCIA

[4-37] En coordinación con el comandante y el estado mayor/plana mayor, el personal de inteligencia y operaciones recibe y evalúa los requerimientos de información, prepara el plan de recolección, le recomienda los medios y disciplinas a emplear al personal de la sección de operaciones y mantiene la sincronización a medida que las operaciones avanzan (MFRE 2-0); en virtud de esto, se podrán desarrollar las siguientes actividades:

- Desarrollar los planes o los requerimientos de sincronización de inteligencia, vigilancia y reconocimiento para satisfacer las solicitudes de recolección de información de CI que necesita el comandante.
- Planear y verificar el desarrollo de las operaciones de CI diseñadas para respaldar las operaciones militares actuales y futuras.
- Garantizar que los requerimientos de recolección de CI sean comunicados de manera efectiva a quienes realizan el procedimiento operacional de CI.
- Hacer seguimiento, monitoreo y evaluación a la efectividad de las actividades de CI y proporcionar datos estadísticos e informes sobre las actividades, según sea necesario.

CI

Contrainteligencia



- Asegurar que los elementos de recolección de información de CI cuenten con la capacidad, los recursos y la infraestructura para cumplir con los requerimientos exigidos.
- Proporcionar información para la sincronización de inteligencia, lo cual requiere el conocimiento de FISS y OT, la disponibilidad de recursos para la recolección, las prioridades de recolección y las áreas geográficas donde se llevará a cabo la actividad.

[4-38] Los planes de inteligencia, vigilancia y reconocimiento deben modificarse con la frecuencia que dicten los eventos, las operaciones militares, los nuevos requerimientos y los cambios a los requerimientos previos debido a la falta de inteligencia. El plan de recolección de CI puede organizarse incluyendo los siguientes elementos:

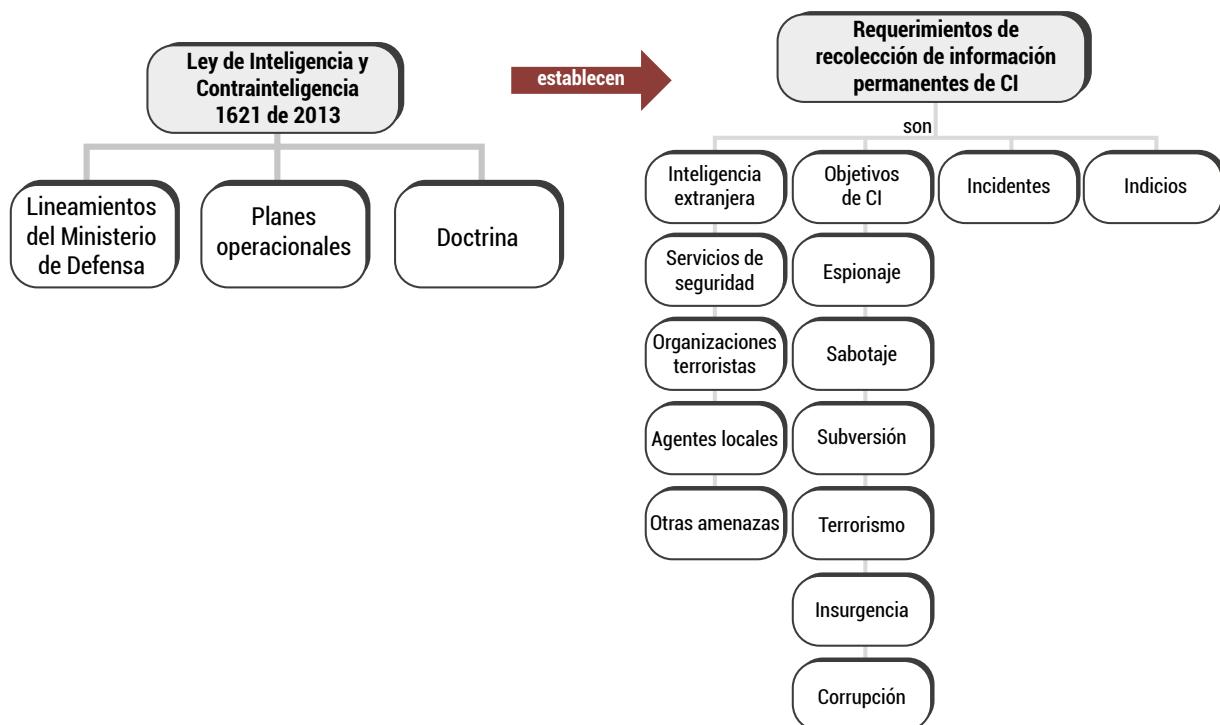
- Misión: identifica los requerimientos de recolección para respaldar una misión o una operación en un área geográfica o un comando.
- Concepto de la operación: identidad del elemento de recolección y enfoque de la recolección.
- Consideraciones operacionales: medidas de seguridad de las operaciones (OPSEC, por su sigla en inglés), medidas de seguridad militar, evaluación de fuentes e información.
- Requerimientos de soporte administrativo: informes, arquitectura de comunicaciones, canales de comunicación.
- Gastos operacionales.

[4-39] Los planes de inteligencia, vigilancia y reconocimiento deben evaluar las capacidades del elemento de recolección de CI, al abordar los siguientes problemas:

- Capacidad: la capacidad del elemento de recolección para satisfacer el requerimiento y la existencia de una fuente que pueda responder al requerimiento.

- Acceso: si el elemento de recolección tiene la capacidad de acceder a la fuente o a la información.
- Recursos: los recursos disponibles para el elemento de recolección, que permitan lograr los objetivos y la identificación de los recursos adicionales.
- Potencial: para la administración de fuentes.
- Prioridades: determinar y evaluar la prioridad de los nuevos requerimientos en comparación con los que se encuentran en desarrollo.

4.6. REQUERIMIENTOS DE RECOLECCIÓN DE INFORMACIÓN PERMANENTES DE CONTRAINTELIGENCIA



| Figura 4-1 | Requerimientos de recolección de información permanentes de CI

CACIM | Comando de Apoyo de Combate de Contra Inteligencia Militar

[4-40] Los requerimientos de recolección de información permanentes de CI, sirven de base para planear e implementar la recolección de CI, encabezados por el CACIM o quien haga sus veces, y teniendo como guía de trabajo lo establecido en la Ley de Inteligencia y Contra Inteligencia 1621 de 2013, el Decreto 1070 de 2015, los lineamientos del Ministerio de Defensa, los planes operacionales, la doctrina y los demás documentos que validen la recolección de información de CI (ver la figura 4-1). La CI dentro de los límites de su misión, de las prioridades asignadas, de los recursos, de la ubicación y de sus capacidades, tiene la obligación de recolectar e informar sobre actividades de las redes de inteligencia de la amenaza, objetivos, incidentes o indicios de CI y cualquier otra información de interés para la disciplina.

4.7. APOYO DE CONTRAINTELIGENCIA A EVALUACIONES DE AMENAZAS Y EVALUACIONES DE VULNERABILIDADES

CI | Contra Inteligencia

[4-41] Las evaluaciones de amenazas y evaluaciones de vulnerabilidades son estudios realizados por agentes de CI para proporcionar a un comando o a una organización apoyada una apreciación de las redes de inteligencia de la amenaza o de la susceptibilidad de la unidad o la agencia a la recolección de información por parte de la amenaza.

FISS | Inteligencia extranjera y servicios de seguridad

[4-42] Las evaluaciones de amenazas se centran en las capacidades de recolección de FISS o de OT conocidas o sospechadas en un AO específica, y pueden utilizarse con fines de planeamiento, de capacitación o de seguridad.

OT | Organizaciones terroristas

[4-43] Las evaluaciones de vulnerabilidad son técnicas o procedimientos independientes que se llevan a cabo con un objetivo específico (por ejemplo: comando, agencia, instalación, operación) y se adaptan a las necesidades de cada solicitante. El objetivo de estas evaluaciones es proporcionar una herramienta realista que valore las actividades de seguridad o de protección interna, para, de esta forma, plantear acciones de mejora para mitigar, contrarrestar o, si es posible, lograr una adecuada explotación del riesgo a favor de la Fuerza. Tales evaluaciones podrán incluir:

- Datos demográficos, políticos, sociales y económicos generales para el área objetivo que pueden ser explotados por un elemento de FISS o de OT.
- Asociaciones conocidas o sospechosas entre los elementos de la inteligencia de la amenaza y las agencias gubernamentales o el personal que pueden indicar apoyo, dirección o financiación de los elementos de la inteligencia de la amenaza.
- Análisis de las variables operacionales.
- Detalles sobre elementos de la inteligencia de la amenaza conocidos o sospechosos (identidades de miembros conocidos, capacidades, planes e intenciones, técnicas o procedimientos implementados por la amenaza).
- Hechos, situaciones o antecedentes de los que la inteligencia de la amenaza ha sido responsable, los que se le han atribuido o los que ha apoyado.
- Evaluación de capacidades de recolección de inteligencia del enemigo.
- Identificación de las vulnerabilidades basadas en el análisis de la información recolectada para efectuar recomendaciones de contramedidas y verificar la efectividad de estas.

FISS | Inteligencia extranjera y servicios de seguridad

OT | Organizaciones terroristas

DEBRIEFING

Actividad que busca obtener información a través de preguntas sistemáticas respecto a un tema particular (MCE 2-22.1).

SONSACAMIENTO

Técnica discreta de entrevista, que no le permite al entrevistado conocer la intención específica del agente (MCE 2-22.1).



CORRUPCIÓN DENTRO DE LA FUERZA

En 2013, se dio inicio a una operación de CI dirigida a un caso de corrupción presentado en la Dirección de Sanidad del Ejército (DISAN) y varios hospitales militares y dispensarios, en todo el país. Esta operación consistió en la identificación de una organización que delinquía dentro del Ejército, la cual estaba conformada por militares activos y retirados, médicos y abogados que se dedicaban a la elaboración fraudulenta de conceptos médicos de usuarios, en los cuales se especificaba que estas personas presentaban un alto porcentaje de pérdida de su capacidad laboral, para así alcanzar de forma ilícita indemnizaciones y pensiones.

Esta operación, que se prolongó durante cinco años, se desarrolló en tres fases. La primera consistió en el empleo de agentes encubiertos para identificar el *modus operandi* de la organización y a las personas involucradas en las acciones ilícitas. La información recolectada fue dejada a disposición de la Fiscalía General de la Nación y permitió la captura de 35 personas involucradas en los actos de corrupción; entre ellas, personal militar activo. En la segunda fase se direccionó la recolección de información a identificar los bienes adquiridos de manera ilegal por las personas que integraban dicha organización, lo cual conllevó una extinción de dominio que alcanzó un valor de 24 mil millones de pesos y permitió la captura de otras 20 personas.

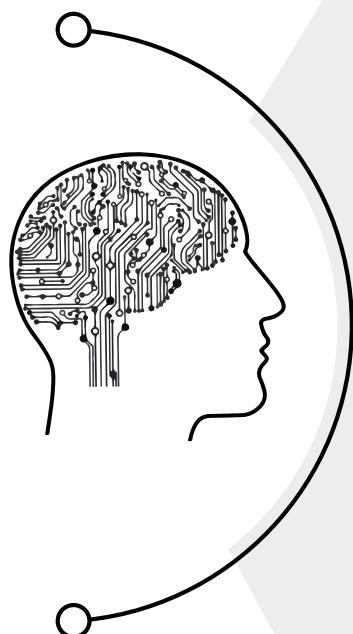
Debido a los resultados que se habían obtenido hasta el momento, se evidenció una disminución en el desfalco presupuestal que se venía presentando a lo largo de los últimos años, lo cual, a su vez, indicaba que los actos de corrupción habían cesado. No obstante, en 2018, la CI logró identificar a otro grupo de personas que seguían desarrollando acciones ilícitas valiéndose esta vez de una nueva modalidad. Esto dio inicio a la tercera fase de la operación, la cual tuvo como resultado la captura de 16 personas más.

CAPÍTULO 5

ANÁLISIS DE CONTRAINTELIGENCIA

"El auténtico genio consiste en la capacidad para evaluar información incierta, aleatoria y contradictoria".

Winston Churchill



- GENERALIDADES 
- ANÁLISIS DE INFORMACIÓN
 - Apreciaciones dinámicas
 - Análisis de amenazas de CI
- ANÁLISIS OPERACIONAL
 - Identificación de anomalías, indicadores y patrones
 - Perfilación de fuentes
- HERRAMIENTAS ANALÍTICAS
 - Diagrama de eventos en el tiempo
 - Matrices
 - Diagrama de análisis de enlace
- APOYO DE LA CI PARA LA PICC
 - Planeamiento operacional
 - Lista de blancos de CI

5.1. GENERALIDADES

[5-1] Para que los comandantes completen eficazmente el proceso de operaciones, deben tener información e inteligencia. El proceso de inteligencia satisface esta necesidad al proporcionar al comandante inteligencia sobre la amenaza, el ambiente operacional y la situación. Cuatro pasos constituyen el proceso de inteligencia: planeamiento y dirección; recolección de información; procesamiento y difusión, y retroalimentación. Además, hay dos actividades que ocurren en los cuatro pasos del proceso de inteligencia: analizar y evaluar. Estas actividades continuas más el impulso del comandante determinan y desarrollan el proceso. Pueden ocurrir en cualquier momento durante el mismo.

[5-2] El análisis implica obtener información útil, emplear la experiencia, las herramientas analíticas, las bases de datos, la integración, la evaluación y la reevaluación de la información, así como el razonamiento, para llegar a una conclusión basada en los hechos, y no en suposiciones. El conocimiento del analista de inteligencia debe abarcar aspectos tales como:

- Conocimiento de las herramientas de análisis de inteligencia y CI.
- Conocimiento de la amenaza y de la fenomenología que pueda afectar la evaluación de la información.
- Interpretación de la inteligencia alcanzada a lo largo del proceso de análisis.
- Conocimiento de las políticas de seguridad de la información.
- Tener en cuenta el uso de la inteligencia y de los canales de comunicación para su difusión.

CI | Contrainteligencia

[5-3] El análisis de información no debe ser tarea exclusiva del analista, sino de todos los agentes, los comandantes y los líderes de CI. Es responsabilidad general ayudar a impulsar las averiguaciones y las operaciones de CI mediante la orientación de las actividades para la recolección de información

de actividades de espionaje, terrorismo, sabotaje, subversión, insurgencia, corrupción o cualquier otra realizada por parte de la amenaza.

[5-4] El análisis de CI implica las acciones tomadas para evaluar la información obtenida por todas las fuentes, a fin de determinar interrelaciones, tendencias y significado contextual. El analista revisa e incorpora, según sea necesario, información de otras disciplinas de la FCG Inteligencia y los análisis de todas las fuentes, para proporcionar una base de entendimiento sólido para su labor. El análisis de CI adelantado mediante única fuente se procesará con la aplicación de las herramientas y los medios disponibles de la disciplina.

[5-5] El análisis es más que, simplemente, reafirmar hechos: dispone de la información para generar alertas de amenazas que puedan afectar a la Fuerza. El análisis de CI utiliza los principios analíticos del procesamiento de las entradas de datos, la factorización de diferentes variables y el desarrollo de una hipótesis, que es la base del análisis predictivo. El analista formula una hipótesis basada en los datos disponibles, evalúa la situación y explica qué significan los datos en términos lógicos que faciliten la comprensión del destinatario. Hay dos procesos de pensamiento básicos utilizados mutuamente por los analistas para estudiar problemas y llegar a conclusiones: inducción y deducción.

[5-6] La inducción es el proceso de formular hipótesis sobre la base de la observación o de otra evidencia. Se la puede caracterizar mejor como un proceso de descubrimiento cuando el analista puede establecer una relación entre los eventos bajo observación o estudio. La inducción, normalmente, precede a la deducción y es el tipo de razonamiento que los analistas deben realizar con más frecuencia.

[5-7] La deducción es el proceso de razonamiento desde reglas generales hasta casos particulares. El analista debe extraer o analizar las premisas para llegar a una conclusión. El razonamiento deductivo, a veces, se denomina *razonamiento demostrativo* porque se usa para demostrar la verdad o la validez de una conclusión basada en ciertas premisas.

FCG	Función de conducción de la guerra
CI	Contrainteligencia

[5-8] El análisis de CI apoya la identificación y la caracterización del componente humano de las operaciones de recolección de inteligencia de la amenaza y sus efectos en las operaciones propias y en las actividades enemigas; además, ayuda al proceso general de todas las fuentes, al identificar acciones específicas y factores motivacionales que fortalezcan el apoyo de la población local o debiliten su apoyo al enemigo al proporcionar información de CI. Además de lo anterior, los analistas:

- Examinan la amenaza actual y potencial para identificar todos los factores, tales como la moral, la motivación, el entrenamiento y las creencias que afectarían positiva o negativamente las capacidades del adversario.
- Identifican a los representantes formales e informales de grupos hostiles, neutrales y amigos, y cómo su influencia puede afectar las operaciones.
- Desarrollan superposiciones, bases de datos y matrices, según sea necesario, para respaldar la PICC.

PICC | Preparación de inteligencia del campo de combate

CI | Contrainteligencia

[5-9] El análisis de CI lleva a cabo el proceso cognitivo de recibir, interpretar e integrar información tomando en cuenta el ambiente operacional. El análisis requiere la organización de la información en categorías y patrones identificables (relaciones entre las categorías), en función de los requerimientos de recolección de información. Los análisis se pueden hacer en cualquier nivel, siempre y cuando sirvan para apoyar la protección de la Fuerza y sus activos críticos. El análisis de CI se divide en análisis de información y análisis operacional.

5.2. ANÁLISIS DE INFORMACIÓN

FISS | Inteligencia extranjera y servicios de seguridad

OT | Organizaciones terroristas

[5-10] El análisis de información de CI es el que cumple, esencialmente, con el tercer paso del proceso de inteligencia. Se encuentra enfocado en el análisis sobre los planes, intenciones y capacidades de FISS, OT, agentes locales y otras amenazas. Una vez se cumple con las actividades de recolección, se procede a hacer el cruce de información con otras fuentes y bases de datos, además de emplear herramientas de análisis

que permitan evaluarla y reevaluarla para que sea integrada y aplicada debidamente. Como resultado de esta actividad, se debe obtener una evaluación de la información y de la fuente; esto le permite al comandante tomar decisiones sobre las tareas de protección por hacer para neutralizar o explotar amenazas a favor del Ejército.

5.2.1. Apreciaciones dinámicas

[5-11] Las apreciaciones dinámicas implican un estudio compuesto que contiene información específica de un área. Es un documento preparado en todo el rango de operaciones militares (ROM), y el cual es refinado y actualizado continuamente. Estas apreciaciones abarcan todos los elementos del ambiente operacional y contribuyen al proceso de la PICC. Los tipos de información contenidos en estas apreciaciones varían según el área. Por lo general, contienen discusiones sobre el despliegue de las fuerzas amigas, las capacidades y las actividades de recolección de la inteligencia de la amenaza, y en ellas se deberán analizar las estructuras, así como las personas clave y los métodos de operación.

[5-12] Las apreciaciones dinámicas implicarán la evaluación de amenazas (análisis de FISS y OT dirigido a identificar los objetivos críticos propios). Dicha evaluación se hace de tal manera que la identificación se logre de forma sencilla; sin embargo, habrá casos en que se requiera un esfuerzo analítico concertado. Los analistas deben concentrarse en identificar los puntos críticos propios, para luego examinar la amenaza conocida o potencial de FISS y OT. Luego se debe evaluar el objetivo respecto a su accesibilidad, su vulnerabilidad y el efecto potencial de su destrucción o su degradación en la efectividad operacional.

CI	Contrainteligencia
PICC	Preparación de inteligencia del campo de combate
FISS	Inteligencia extranjera y servicios de seguridad
OT	Organizaciones terroristas

5.2.2. Análisis de amenazas de contrainteligencia

[5-13] El analista de CI usa las herramientas y las habilidades de análisis centrándose en "cómo vemos al adversario" y en "cómo nos ve el adversario"; a su vez, se enfoca en cómo

contrarrestar los esfuerzos de recolección de información de la amenaza.

[5-14] El análisis y la producción de CI se centran en las actividades de recolección de información de la amenaza que incluyen inteligencia humana (HUMINT, por su sigla en inglés), inteligencia de señales (SIGINT, por su sigla en inglés), inteligencia geoespacial (GEOINT, por su sigla en inglés) e inteligencia técnica (TECHINT, por su sigla en inglés). El enfoque del análisis de CI de cada una de estas disciplinas se refiere no solo a la entidad o las entidades del enemigo que operan en el área, sino también, a los productos de inteligencia que con mayor probabilidad se están desarrollando a través de sus actividades de recolección.

[5-15] Si bien el análisis es un proceso puramente cognitivo, la capacidad de organizar y procesar datos para maximizar la eficiencia de este debe ser totalmente automática (almacenamiento de datos, clasificación y archivo). El proceso de contrarrestar cada una de estas disciplinas implica: evaluación de amenazas, evaluación de vulnerabilidades y desarrollo, implementación y evaluación de contramedidas.

CI | Contrainteligencia

HUMINT | Inteligencia humana

5.2.2.1. Análisis de contrainteligencia humana

[5-16] El esfuerzo de análisis de CI debe tratar de identificar la HUMINT de la amenaza, personas y actividades empleadas para la recolección de información. A fin de entregar un producto completo, el analista de CI puede necesitar acceso a datos e información y hacer requerimientos de información sobre las acciones de la amenaza, en cuanto a subversión, espionaje, sabotaje, terrorismo, insurgencia y cualquier otra acción que pretenda afectar el desarrollo de las operaciones y los activos críticos del Ejército.

SIGINT | Inteligencia de señales

5.2.2.2. Análisis de contrainteligencia de señales

[5-17] El analista de CI requiere el conocimiento de recolección de SIGINT para respaldar la evaluación de vulnerabilidades y contramedidas. La validación de vulnerabilidades (posibles

datos recolectados por la amenaza mediante SIGINT) y la efectividad de las contramedidas implementadas (una comparación antes y después de las contramedidas) será casi imposible sin una recolección activa y oportuna como requisito previo para el análisis. El analista de CI requiere una base de datos que contenga el conocimiento de sistemas de SIGINT, de instalaciones, de técnicas, de procedimientos y de datos del proceso de SIGINT de la amenaza.

[5-18] Además de lo anterior, todas las bases de datos y la información producida por las funciones y las competencias distintivas deberán estar disponibles, así como una base de datos de contramedidas, con un historial de las que han sido implementadas y de los resultados obtenidos previamente. En condiciones ideales, el analista de CI debe, en cualquier momento, ser capaz de anticipar la actividad de amenaza SIGINT; sin embargo, para lograrlo debe basarse en otras recolecciones de CI, HUMINT y GEOINT, así como en el acceso a los archivos de CI de la unidad apoyada.

5.2.2.3. Análisis de constrainteligenzia geoespacial

[5-19] Este tipo de análisis requiere que el analista tenga un conocimiento de los planes, intenciones y capacidades de GEOINT de las redes de inteligencia enemigas. El analista debe tener acceso a todos los datos e inteligencia disponibles sobre la metodología, los sistemas y el procesamiento de GEOINT, así como a la información detallada sobre los sistemas de satélites comerciales y su disponibilidad para el consumidor nacional y extranjero.

[5-20] El analista intenta definir la plataforma de imágenes específica implementada contra los asociados de la AU y el proceso usado para la recolección de GEOINT. El conocimiento del proceso de inteligencia de la amenaza para atacar es crítico en el desarrollo de contramedidas destinadas a derrotar, destruir o engañar a la GEOINT enemiga.

[5-21] Las actividades de GEOINT de la Fuerza deberán también estar orientadas a las actividades de HUMINT del enemigo (grabadoras de video digital, cámaras de teléfonos celulares,

SIGINT	Inteligencia de señales
CI	Contrainteligenzia
HUMINT	Inteligencia humana
GEOINT	Inteligencia geoespacial
AU	Acción unificada

aplicaciones georreferenciadas); la CI deberá recolectar ese tipo de datos para ser analizados.

5.2.2.4. Análisis de contrainteligencia técnica

TECHINT	Inteligencia técnica	[5-22] El analista de CI requiere tener acceso a la recolección de datos de TECHINT para desarrollar contramedidas que permitan negar el uso de las ventajas tecnológicas de un adversario, y permitan así validar las vulnerabilidades detectadas (datos con capacidad de recolección por amenaza TECHINT) y la eficacia de las contramedidas aplicadas; sin embargo, su actividad deberá valerse de una recolección activa y oportuna como un requerimiento previo para el análisis. El analista de CI necesita una base de datos relacional integral que consista en sistemas, capacidades y metodología de amenaza TECHINT.
CI	Contrainteligencia	[5-23] La información sobre amenazas TECHINT debe ser fácilmente accesible desde elementos de inteligencia propios para ayudar a proporcionar una evaluación completa, pero esta actividad requiere el apoyo de otros insumos de información obtenidos por CI, HUMINT, SIGINT y GEOINT.
HUMINT	Inteligencia humana	
SIGINT	Inteligencia de señales	
GEOINT	Inteligencia geoespacial	

5.3. ANÁLISIS OPERACIONAL

[5-24] El análisis operacional permite medir la efectividad del personal, los equipos, las técnicas y los procedimientos empleados en las operaciones de CI, así como la medición de la producción de las fuentes (cantidad y calidad de la información), el manejo de las fuentes, la aplicación de técnicas de encubrimiento, entre otros. El análisis operacional permite a los comandantes proporcionar dirección y orientación para aumentar la eficiencia y corregir errores en la ejecución de tareas u operaciones de CI.

[5-25] Este tipo de análisis se utiliza para dirigir las operaciones de CI, responder los requerimientos de información, guiar y recomendar la utilización de técnicas y procedimientos de CI. Se deberá establecer una lista de indicadores priorizados

para responder los RICC y los EEIPT, los cuales permitirán identificar los cursos de acción de la amenaza o sus intenciones.

[5-26] Se deberán coordinar las operaciones o actividades de recolección de información de CI, con las diferentes disciplinas de la FCG Inteligencia, para de esta forma eliminar la superposición innecesaria y la duplicidad de esfuerzos.

[5-27] El control y guía de todas las actividades de CI, está bajo el control y dirección de los comandantes de CI, en cada nivel del mando y son ellos los que tienen la responsabilidad de realizar el análisis operacional, con el fin de:

- Identificar los vacíos de información y guiar la recolección de información.
- Administrar fuentes e informantes.
- Manejar la información de CI.
- Proporcionar información a los comandantes para responder a los requerimientos de información.
- Guiar la recolección de información de las unidades subordinadas.
- Preparar y entrenar al personal para el cumplimiento de actividades dentro de las operaciones de CI.

[5-28] Por otro lado, los RICC y los EEIPT deben ser respondidos por la CI, dentro de la organización del estado mayor o plana mayor. El deberá guiar la recolección de información para:

- Satisfacer los requerimientos del comandante.
- Sincronizar la CI con las otras disciplinas de inteligencia.
- Garantizar la seguridad de los agentes y de la información.
- Mantener el flujo de información tanto para el comandante militar, como para el comandante de CI.

RICC	Requerimientos de información crítica del comandante
EEIPT	Elementos esenciales de información de las propias tropas
CI	Contrainteligencia

[5-29] Para desarrollar el análisis operacional de contrainteligencia se deberán tener en cuenta dos aspectos esenciales: la identificación de anomalías, indicadores y patrones, y la perfilación de fuentes.

5.3.1. Identificación de anomalías, indicadores y patrones

[5-30] Un componente crítico del análisis operacional de CI es la incorporación de diferentes anomalías, indicadores o patrones que pueden ser señales de la focalización de recolección de información por parte de la amenaza.

[5-31] Las anomalías son actividades irregulares o inusuales que pueden incitar sospecha acerca de una actividad anormal. El analista de CI puede presumir que existe una recolección de información por parte de la amenaza. Las anomalías pueden consistir en pruebas repetidas, pero sutiles, de procedimientos sistemáticos o de seguridad.

[5-32] Los indicadores son manifestaciones de posibles técnicas o procedimientos de recolección de información por parte de la amenaza, incluida la vigilancia de las instalaciones.

CI | Contrainteligencia

[5-33] Los patrones son incidentes repetidos que pueden ser de naturaleza similar o eventos diferentes que ocurren en un lugar o un periodo específico, y que pueden indicar posibles ataques de la inteligencia de la amenaza o explotación de información.

[5-34] El análisis de anomalías, indicadores y patrones puede ayudar a impulsar las actividades de CI y desarrollar operaciones para negar, mitigar, degradar o explotar las actividades de recolección de la inteligencia de la amenaza.

PMTD | Proceso militar para la toma de decisiones

5.3.2. Perfilación de fuentes

[5-35] A través de la perfilación de fuentes se evalúa qué tipo de persona puede satisfacer los requerimientos de información permanentes para respaldar el PMTD del comandante.

Si bien hay connotaciones negativas asociadas con el "perfil", los perfiles de las fuentes están diseñados para maximizar el tiempo y los recursos de CI. El desarrollo de un perfil de fuentes es una herramienta de planeamiento que puede desarrollar la CI para su enfoque operacional.

[5-36] Teniendo en cuenta el estudio de las fuentes y su origen, la CI, a través de perfiles de fuentes, puede planear misiones para poner a su personal en ambientes donde es más probable que entren en contacto con alguien que pueda responder a un requerimiento. Una vez se encuentre en ese ambiente, la CI puede evaluar con rapidez las fuentes durante las operaciones y priorizar a las personas que sean una fuente potencial de información. El perfil de las fuentes debe tener en cuenta las siguientes variables para identificar la fuente óptima que satisfaga los requerimientos de información:

- **Demografía:** ¿qué origen étnico, afiliación, edad o profesión de una fuente podría satisfacer el requerimiento de información basado en la situación o el AO?
- **Ubicación:** la proximidad de la fuente potencial en relación con el entorno donde podría obtener la información (geográficamente, culturalmente).
- **Acceso:** la capacidad de una fuente para obtener información directa o indirecta que satisfaga un requerimiento.
- **Motivación:** las convicciones, las ideologías o los incentivos compensatorios que induzcan a una persona a cooperar y a proporcionar información a un agente de CI del Ejército.
- **Controlar:** los rasgos de carácter o los atributos de una fuente que le permitirían responder a la dirección de los agentes.

CI | Contra Inteligencia

AO | Área de operaciones

VARIABLES PARA IDENTIFICAR LA FUENTE ÓPTIMA



CI | Contra Inteligencia

5.4. HERRAMIENTAS ANALÍTICAS

[5-37] El análisis de CI utiliza herramientas para archivar, agrupar y correlacionar datos y, de esta forma, generar productos de análisis basados en una metodología específica. Algunas herramientas también se pueden usar para representar gráficamente la información, y así facilitar la comprensión por parte del receptor. Existen tres herramientas de análisis que son útiles para el análisis de CI cuando esta actúa como una sola disciplina. Estas herramientas son:

- Diagrama de eventos en el tiempo.
- Matrices.
- Diagrama de análisis de enlaces.

[5-38] Cada una de estas herramientas toma fragmentos de información y los organiza para crear un gráfico que facilita el entendimiento. Los tratadores de información y analistas de CI pueden usar diferentes tipos de *software* para producir estas herramientas o pueden crearlas en papel.

5.4.1. Diagrama de eventos en el tiempo

[5-39] Un gráfico de eventos en el tiempo es un método para ubicar y representar cronológicamente acciones individuales o grupales de la amenaza. Utiliza símbolos para representar eventos, fechas y el flujo de tiempo. Normalmente, los triángulos se usan para representar el principio y el final del gráfico y se pueden usar dentro del gráfico para indicar eventos particularmente críticos. Los rectángulos, utilizados como nodos de eventos, almacenan datos administrativos e indican eventos o actividades importantes. Dibujar una "X" a través del nodo de evento puede resaltar eventos notables o importantes.

HERRAMIENTAS ANALÍTICAS

Diagrama de eventos en el tiempo

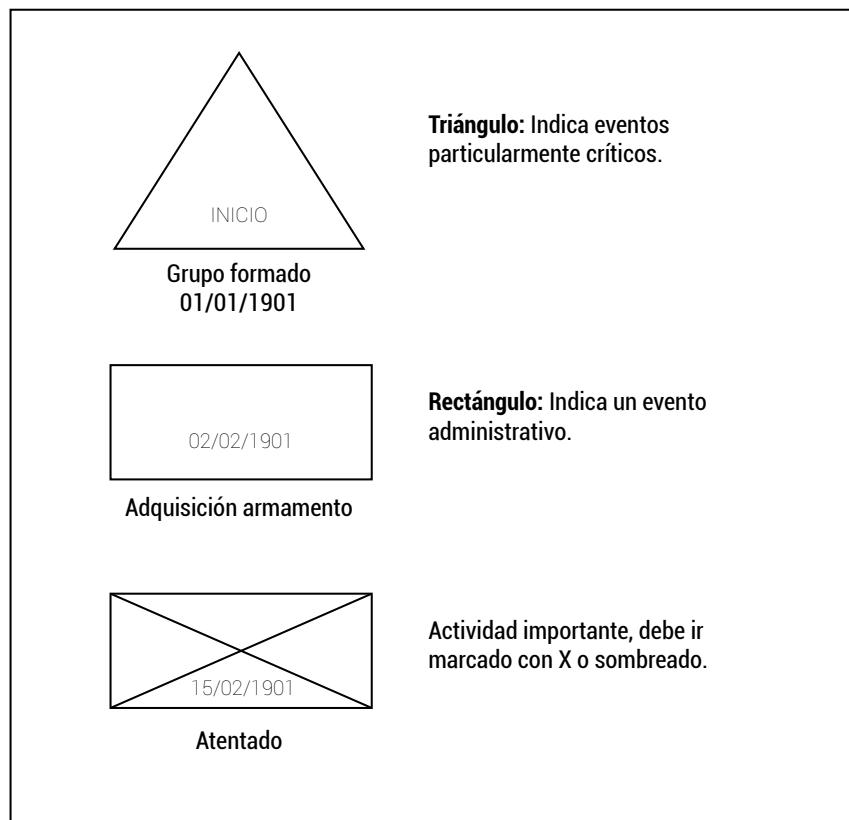
Matrices

Diagrama de análisis de enlaces

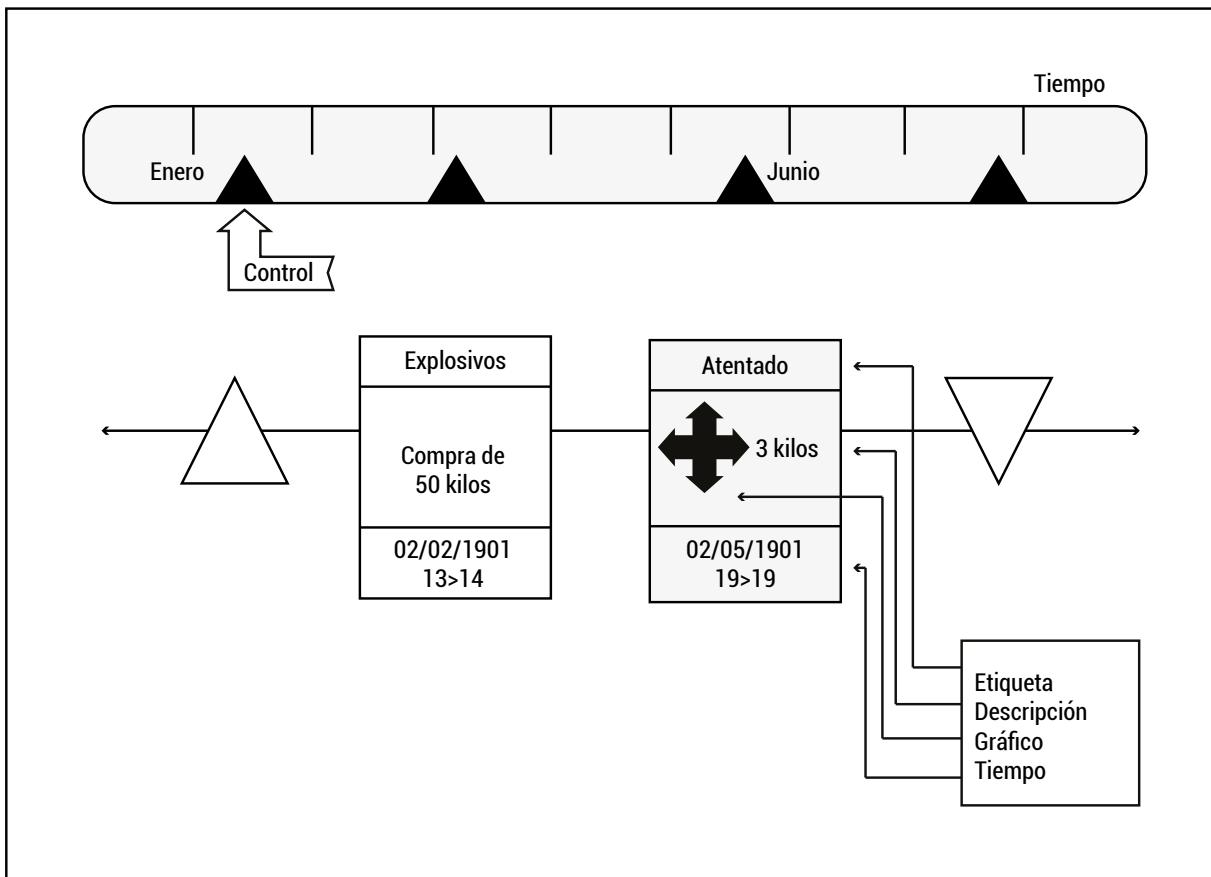
[5-40] Cada uno de estos símbolos contiene un número de secuencia, fecha (día, mes y año del evento), y, si se quiere, puede contener un número de referencia de archivo. La descripción

del incidente escrita debajo del nodo del evento es una breve explicación de este, incluyendo el tipo de incidente. Las flechas indican el flujo de tiempo.

[5-41] Al usar estos símbolos y descripciones breves, es posible analizar las actividades, las transiciones, las tendencias y, en particular, los patrones del grupo, tanto en tiempo como en actividad. Si así se quiere, los nodos de evento pueden estar codificados por colores para indicar un evento o un tipo de evento particular, y así facilitar el reconocimiento de patrones. El gráfico de eventos de tiempo es la mejor herramienta analítica para el análisis de patrones. La figura 5-1 muestra un ejemplo de gráfico de eventos en el tiempo como los grafica el analista. La figura 5-2, por su parte, presenta un ejemplo de la simbología utilizada para crear un gráfico de eventos en el tiempo.



| Figura 5-1 | Ejemplo de gráfico de eventos en el tiempo



| Figura 5-2 | Ejemplo para la simbología en gráficos de eventos en el tiempo

5.4.2. Matrices

[5-42] La construcción de una matriz es una forma sencilla de mostrar las relaciones entre una cantidad de elementos asociados, similares o diferentes. Uno de dichos elementos puede ser cualquiera que sea importante para un esfuerzo de recolección, como personas, lugares, organizaciones, armas, matrículas de automóviles, números de teléfono o ubicaciones, entre otros elementos que resulten importantes para el análisis.

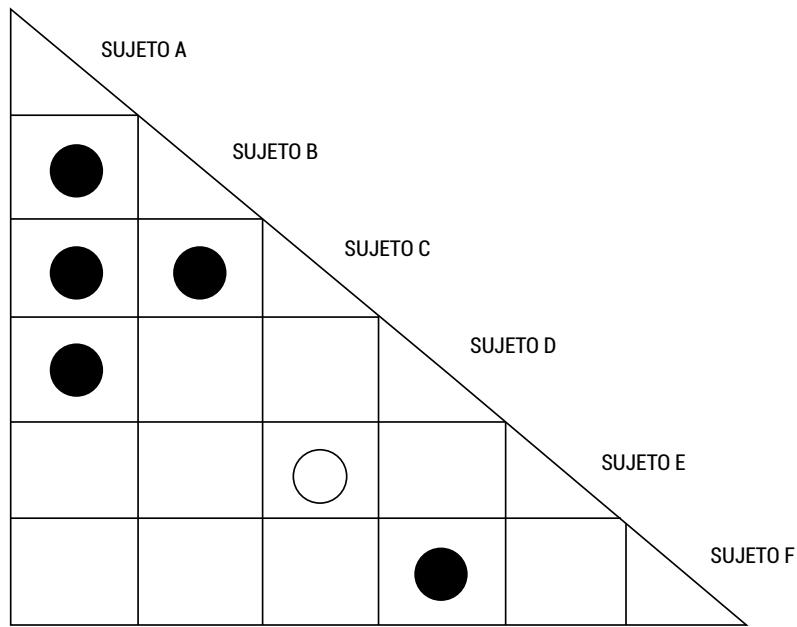
[5-43] En el análisis, las matrices se usan a menudo para identificar "quién sabe quién", "quién ha estado en..." o "quién ha hecho qué" de una manera clara y concisa. Hay dos tipos de matrices utilizadas en el análisis humano:

- Matriz de asociación: utilizada para determinar la existencia de relaciones entre personas (individuales).
- Matriz de actividades: utilizada para determinar la conectividad entre individuos y cualquier organización, evento, dirección, actividad o cualquier otra entidad no personal.

[5-44] Los gráficos involucrados en la construcción de los dos tipos de matrices difieren ligeramente, pero los principios son idénticos.

5.4.2.1. Matriz de asociación

[5-45] Una matriz de asociación muestra las conexiones entre las personas clave involucradas en cualquier evento o actividad. Muestra asociaciones dentro de un grupo o de una actividad asociada. Usualmente, este tipo de matriz se construye en forma de un triángulo equilátero que tiene el mismo número de filas y columnas. Las personas se deben enumerar exactamente en el mismo orden a lo largo de las filas y las columnas, para garantizar que todas las asociaciones posibles se representen correctamente. Un método alternativo es enumerar los nombres a lo largo del lado diagonal de la matriz. Este tipo de matriz no muestra la naturaleza, ni el grado ni la duración de una relación: tan solo muestra que existe una relación. El propósito de la matriz (ver la figura 5-3) es mostrarle al analista "quién conoce a quién" y "de quién se sospecha que sabe qué". En caso de que una persona de interés fallezca, se dibuja un rombo junto al nombre del difunto en la matriz.



| Figura 5-3 | Matriz de asociación (el sujeto A tiene relación comprobada con los sujetos B, C y D)

[5-46] El analista usa un círculo cerrado (relleno) para representar una asociación fuerte o conocida, como se muestra en la figura 5-3. Una asociación conocida se determina por contacto directo entre una o más personas.

[5-47] El contacto directo está determinado por varios factores. Las asociaciones directas incluyen:

- Reuniones cara a cara.
- Conversaciones telefónicas en las que el analista está seguro de quién estaba conversando con quién.
- Miembros de una célula u otro grupo que están involucrados en las mismas actividades.

[5-48] Las asociaciones sospechosas o débiles, en las que existen indicadores bajos de asociación y no es posible confirmar un vínculo, se representan con un círculo abierto (sin relleno). Ejemplos de asociaciones sospechosas son:

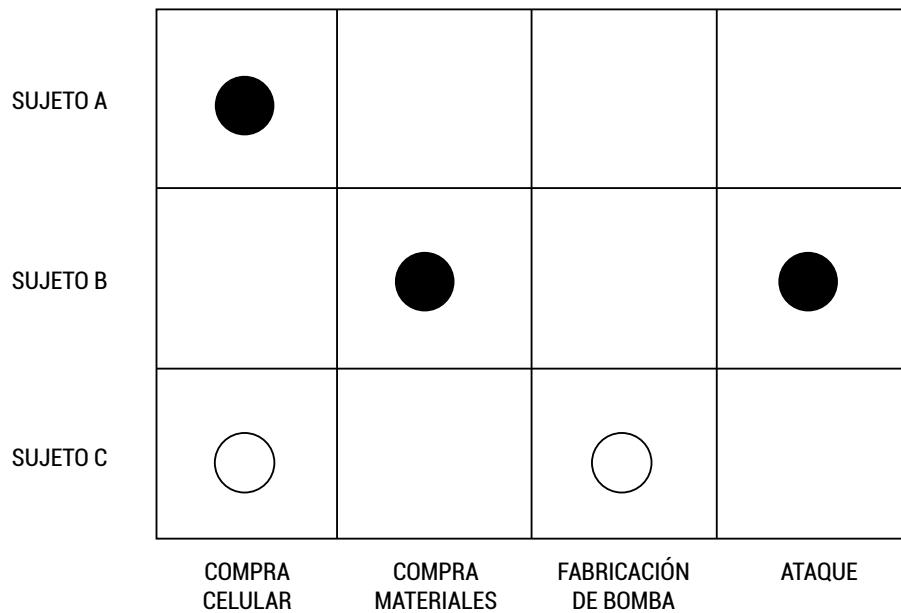
- Una persona plenamente identificada que llama a un número de teléfono perteneciente a una organización al

margen de la ley, pero no se puede determinar con certeza qué persona contestó la llamada.

- Una reunión cara a cara en la que se puede identificar a una de las partes, pero a la otra parte solo se la puede identificar relativamente.

[5-49] La justificación para representar asociaciones sospechosas es acercarse lo más posible a una solución analítica objetiva mientras se permanece lo más cerca posible de hechos conocidos o confirmados. Si una asociación sospechada se confirma posteriormente, se puede hacer el ajuste apropiado en la matriz de asociación. Una razón secundaria para representar asociaciones sospechosas es que puede darle al analista un enfoque para asignar recursos limitados a recolecciones de inteligencia para confirmar la asociación sospechosa. Un punto importante para recordar sobre el uso de la matriz de asociación es que sin modificaciones solo mostrará la existencia de relaciones, y no la naturaleza, ni el grado o la duración de esas relaciones.

5.4.2.2. Matriz de actividades



| Figura 5-4 | Diagrama de análisis de enlaces

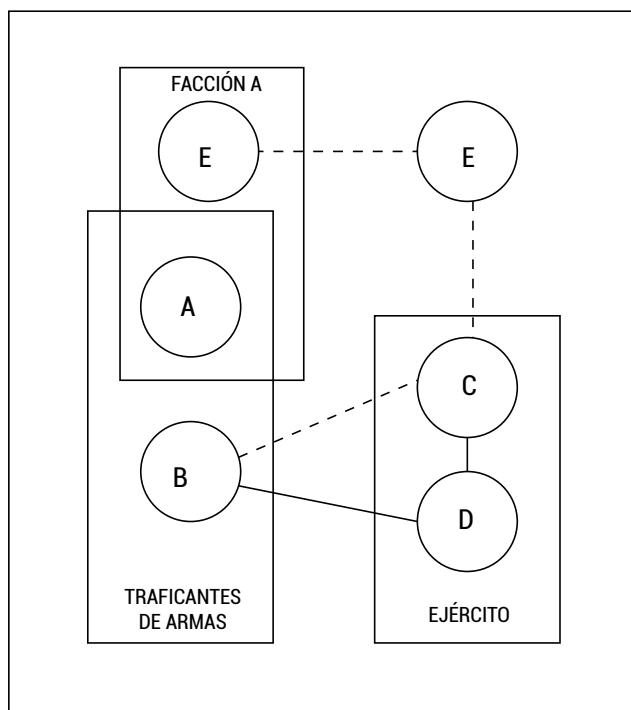
[5-50] La figura 5-4 muestra una matriz rectangular de personas comparada con actividades, ubicaciones, eventos u otra información. El tipo y la calidad de los datos disponibles para el recolector determinan el número de filas y de columnas, así como su contenido. El analista puede adaptar la matriz para ajustarse a las necesidades del problema en cuestión o agregar a ella a medida que el problema se expande en alcance. Esta matriz, normalmente, se construye con nombres de personas ordenadas, en una lista vertical en el lado izquierdo de la matriz, con eventos, actividades, organizaciones, direcciones o cualquier otro denominador común dispuestos a lo largo de la parte inferior de la matriz.

[5-51] La matriz de actividades es fundamental para el estudio de las actividades internas y externas de un grupo, así como de vínculos, de lazos externos, e, incluso, del *modus operandi*. Al igual que con la matriz, las asociaciones confirmadas, o "fuertes", entre individuos y entidades no personales se muestran con un círculo cerrado (relleno), mientras que las asociaciones sospechosas, o "débiles", se ilustran mediante un círculo abierto (sin relleno).

[5-52] Mediante el uso de matrices, el analista puede identificar los objetivos óptimos para una mayor recolección de información y para identificar personas clave dentro de una organización, y así aumentar considerablemente la comprensión del analista sobre una organización y su estructura. Las matrices se pueden usar para presentar resúmenes o para almacenar información de una manera concisa y comprensible dentro de una base de datos. Las matrices aumentan la comprensión, pero no pueden reemplazar los procedimientos operacionales estandarizados ni los archivos de bases de datos. Es posible, y algunas veces productivo, usar una matriz para todas las asociaciones.

5.4.3. Diagrama de análisis de enlaces

[5-53] El diagrama de análisis de enlaces muestra las conexiones entre personas, grupos o actividades. La diferencia entre las matrices y el análisis de enlaces es aproximadamente la misma que la diferencia entre un cuadro de kilometraje y un mapa de ruta. El cuadro de kilometraje (matriz) muestra las conexiones entre las ciudades que usan números para representar las distancias de viaje y el mapa de ruta (diagrama de análisis de enlaces) utiliza símbolos que representan ciudades, ubicaciones y carreteras para mostrar cómo dos o más ubicaciones están vinculadas entre sí. La figura 5-5 es un ejemplo de un diagrama de análisis de enlaces.

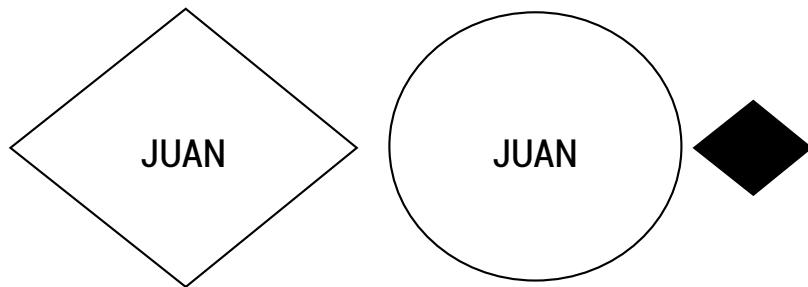


| Figura 5-4 | Matriz de actividades

[5-54] Al igual que con la construcción de matrices de asociación, hay ciertas reglas de gráficos, de simbología y de construcción que deben seguirse. La estandarización es fundamental para garantizar que todos los que construyen,

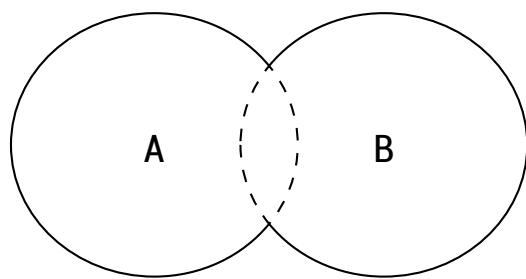
usan o leen un diagrama de análisis de enlaces comprendan exactamente lo que muestra dicho diagrama. Los círculos y las líneas están dispuestos de modo que no se crucen líneas, siempre que sea posible. A menudo, especialmente cuando se trata de grupos grandes, es muy difícil construir un diagrama de líneas en el que estas no se crucen. En estos casos, se debe hacer todo lo posible por mantener el número de cruces en un mínimo requerido. Las reglas estándar que se deben seguir al respecto son:

[5-55] Las personas se muestran como círculos abiertos (sin relleno), con el nombre escrito dentro del círculo. Las personas difuntas se representan en círculos abiertos (sin relleno), con un rombo al lado del círculo, que representa a esa persona (ver la figura 5-6), o rombos abiertos (sin relleno) con el nombre escrito dentro de él.



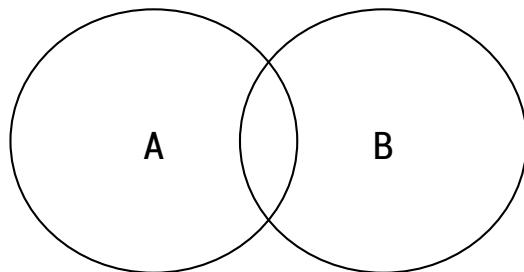
| Figura 5-6 | Ejemplo de graficación de persona fallecida

[5-56] Las personas conocidas por más de un nombre (seudónimos) se muestran como círculos superpuestos, con nombres en cada círculo.



| Figura 5-7 | Ejemplo para persona con varios seudónimos no confirmados

[5-57] Si se sospecha el alias, se usa una línea de puntos para representar la intersección (ver la figura 5-7). Si se confirma el alias, la intersección se muestra con una línea continua (ver la figura 5-8).



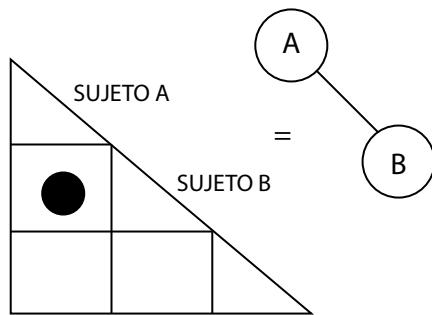
| **Figura 5-8** | Ejemplo para persona con varios seudónimos confirmados

[5-58] Las entidades no personales (organizaciones, eventos, ubicaciones) se muestran como rectángulos adecuadamente etiquetados (ver la figura 5-9).



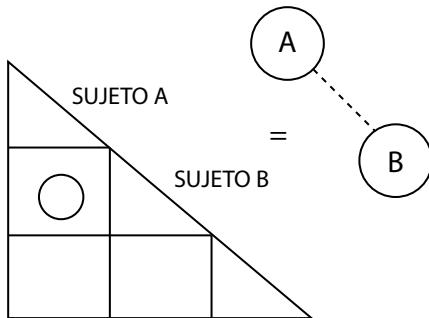
| **Figura 5-9** | Ejemplo de entidad no personal

[5-59] Las líneas continuas (ver la figura 5-10) denotan enlaces o asociaciones confirmadas.



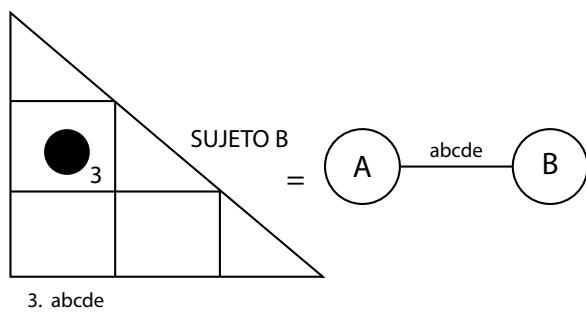
| **Figura 5-10** | Asociaciones confirmadas

[5-60] Las líneas punteadas (ver la figura 5-11) muestran vínculos y asociaciones sospechosas.



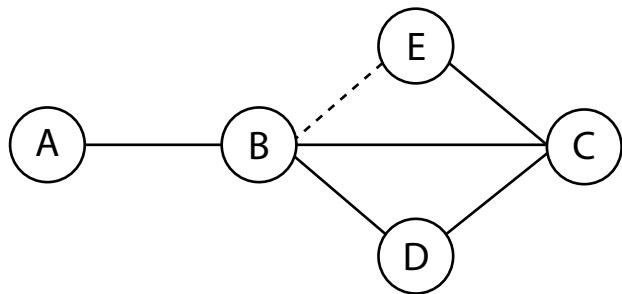
| Figura 5-11 | Asociaciones no confirmadas

[5-61] Las notas al pie se pueden mostrar como una breve leyenda en la línea de conectividad (ver la figura 5-12).



| Figura 5-12 | Leyenda en la línea de conectividad

[5-62] Cada persona o entidad no personal se representa solo una vez en un diagrama de análisis de enlaces. La figura 5-13 muestra solo conectividad entre personas.



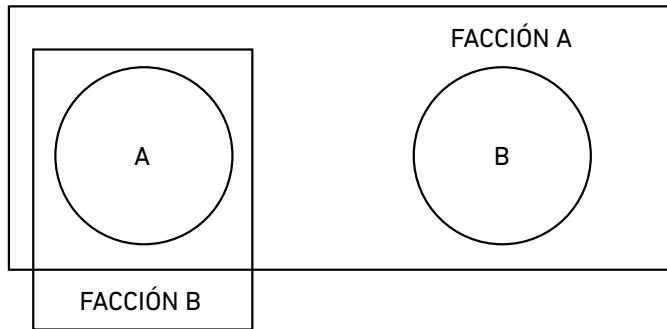
| **Figura 5-13 |** Conectividad entre personas

[5-63] El analista puede determinar fácilmente, a partir del diagrama, que Alpha conoce a Bravo, y que Bravo conoce a Charlie y a Delta. Se sospecha que Bravo conoce a Echo, y Charlie conoce a Delta, Bravo y Echo. Aunque la misma información podría mostrarse en una matriz, es más fácil de entender cuando se la representa en un diagrama de análisis de enlaces. A medida que las situaciones o las averiguaciones se vuelven más complejas, la facilidad para comprender un diagrama de análisis de enlaces se hace más evidente. En casi todos los casos, la información disponible se representa y se analiza primero en ambos tipos de matrices, que luego se utilizan para construir un diagrama de análisis de enlaces para su posterior análisis.

[5-64] Los diagramas de análisis de enlaces pueden mostrar organizaciones, miembros dentro de la organización, equipos de acción, células o participantes en un evento. Como cada individuo representado en un diagrama de análisis de enlaces puede mostrarse solo una vez y algunas otras personas pueden pertenecer a más de una organización o participar en más de un evento, es posible que los rectángulos que representan entidades no personales se superpongan.

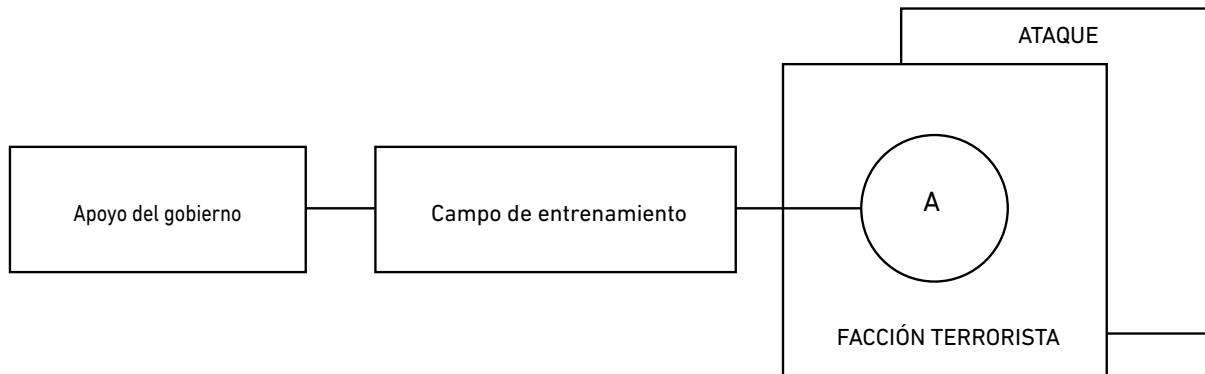
[5-65] Hay más en las organizaciones superpuestas de lo que es inmediatamente obvio. A primera vista, la superposición indica solo que un individuo puede pertenecer a más de una organización o haber participado en múltiples actividades. Un

mayor estudio y análisis revelaría conexiones entre organizaciones, conexiones entre eventos o conexiones entre organizaciones y eventos, ya sea directamente o a través de personas. El diagrama de la figura 5-14 revela una conexión más compleja entre las organizaciones y el personal, demuestra que A y B son ambos miembros de la "Facción A", y que A también es miembro de la "Facción B". Además, dado que A y B se muestran en la misma "caja", es un hecho que están mutuamente asociados.



| Figura 5-14 | Ejemplo de asociación mutua

[5-66] El diagrama de análisis en la figura 5-15 muestra una conexión entre eventos y organizaciones a los cuales un individuo pertenece o está asociado. En este caso, un gobierno dirige un campo de entrenamiento para terroristas. El sujeto A es un miembro de una facción terrorista, está asociado con el campo de entrenamiento y participó en el ataque. A partir de este diagrama, se puede vincular el apoyo del gobierno con el bombardeo (ataque) a través del campamento y el miembro de la facción terrorista.



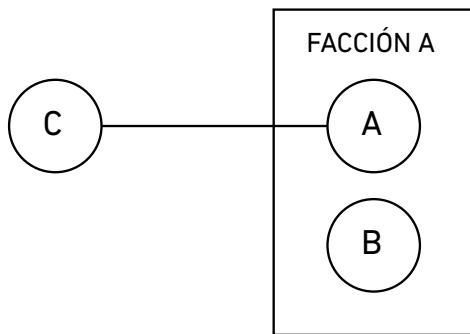
| **Figura 5-15** | Conexión entre eventos y organizaciones

[5-67] Cuando, como suele ser el caso, una organización o un incidente representados en un diagrama de análisis de enlaces contienen los nombres de más de un individuo, no es necesario trazar una línea sólida entre esos individuos para indicar la conectividad. Se supone que los miembros individuales de la misma célula o los participantes en la misma actividad se conocen entre sí; por lo tanto, la conexión entre ellos está implícita. Si las personas no están mutuamente asociadas, no pueden ponerse en la misma "caja". Se debe encontrar otra solución para representar la situación; es decir, mostrar a las personas como asociadas a una organización o una actividad subordinada o diferente.

[5-68] Un conjunto final de reglas para los diagramas de análisis de enlaces se refiere a la conectividad entre individuos que no son miembros de una organización o participantes en una actividad, pero que, de alguna manera, están conectados a esa entidad. Existen dos posibilidades:

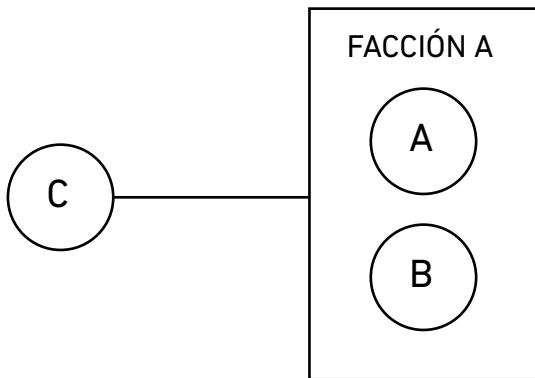
1. El individuo conoce a un miembro o a miembros de la organización, pero no está asociado a la organización misma.
2. La persona está de alguna manera conectada con la organización o actividad, pero no se lo puede vincular directamente con ningún miembro en particular de esa entidad.

[5-69] En el primer caso, la línea de conectividad se dibuja solo entre las personas asociadas como se muestra en la figura 5-16.



| Figura 5-16 | Conectividad entre personas, pero no con la organización

[5-70] En el segundo caso, donde C está asociado a la entidad, pero no las personas que son miembros de la entidad, la situación se muestra como se muestra en la figura 5-17.



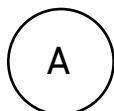
| Figura 5-17 | Conectividad con la organización

[5-71] Los pasos para construir un diagrama de análisis de enlaces son:

- **Paso 1.** Los datos brutos, o fragmentos de información, están organizados en orden lógico. Los nombres de personas, organizaciones, eventos y ubicaciones se compilan en

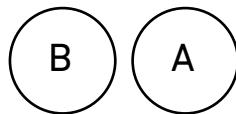
listas apropiadas. En este punto, se puede completar una tabla de eventos de tiempo para ayudar a comprender la información y organizar los eventos en orden cronológico.

- **Paso 2.** La información se ingresa en las matrices apropiadas, mostrando gráficamente "quién está asociado a quién" y "quién está asociado a qué".
- **Paso 3.** Se dibuja la información de la base de datos y de los informes, así como las relaciones de las matrices, pues así se puede construir el diagrama de análisis de enlaces. El mejor método para comenzar el diagrama de análisis de enlaces es:
 - Comience con la matriz de asociación y determine qué persona tiene el mayor número de asociaciones personales. Represente a esa persona en el centro de la página (ver la figura 5-18)



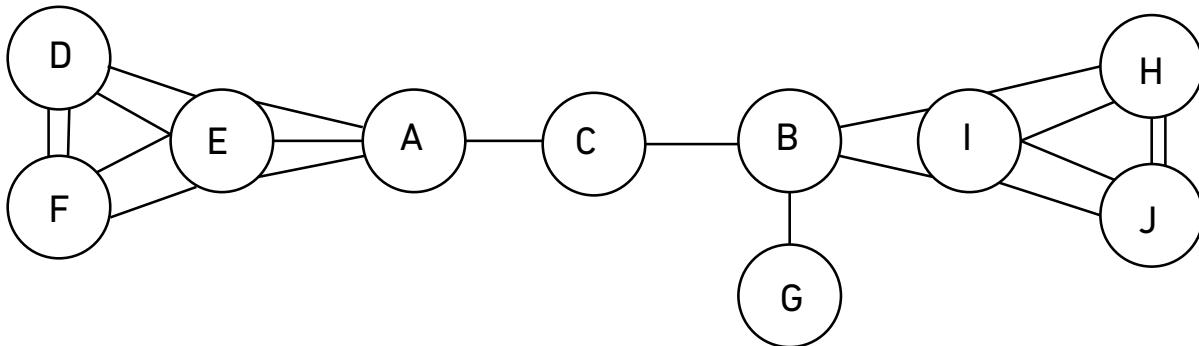
| **Figura 5-18** | Persona con mayor número de asociaciones

- Determine qué persona tiene la segunda cantidad más alta de asociaciones personales. Represente a esa persona cerca de la primera persona como se muestra en la figura 5-19.



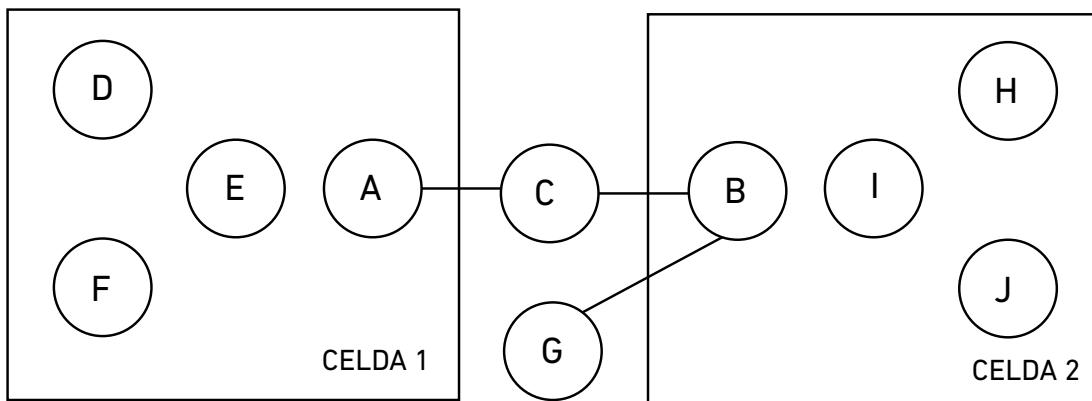
| **Figura 5-19** | Persona con el segundo número más alto de asociaciones personales

[5-72] Use la matriz de asociación donde se muestran todas las asociaciones personales confirmadas y sospechadas (ver la figura 5-20).



| Figura 5-20 | Asociaciones personales

[5-73] Después de que se hayan mostrado todas las asociaciones personales en el diagrama de análisis de enlaces, el analista usa la matriz de actividades para determinar qué actividades, organizaciones y relaciones no personales deben representarse mediante rectángulos apropiados (ver la figura 5-21). Una vez hecho esto, las líneas de conectividad entre personas dentro de los rectángulos pueden eliminarse para evitar el desorden (se entiende que los participantes en la misma actividad o los miembros de la misma célula están relacionados).



| Figura 5-21 | Ejemplo de actividades, organización y relaciones

[5-74] Después de completar las matrices y el diagrama de análisis de enlaces, el analista hace recomendaciones sobre la estructura del grupo y puede identificar las áreas objetivo para una posterior recolección de información. Estas recomendaciones se emplean para verificar las conexiones sospechosas y a las personas clave, y para corroborar o refutar las conclusiones y las evaluaciones extraídas del análisis de enlaces que se ha llevado a cabo. El diagrama de análisis de enlaces y el análisis exhaustivo de la información que contiene pueden revelar mucho sobre una organización. Puede identificar el liderazgo del grupo, así como sus puntos fuertes y débiles y los patrones. El analista puede usarlos para anticiparse a las actividades del enemigo.

5.5. APOYO DE CONTRAINTELIGENCIA PARA LA PREPARACIÓN DE INTELIGENCIA DEL CAMPO DE COMBATE

[5-75] La CI apoya a la PICC al proporcionar productos de la recolección de información sobre la inteligencia extranjera y servicios de seguridad, OT, agentes locales y otras amenazas que impactan el PMTD. El aporte de la CI a la PICC también ayuda en el PSPB y puede dar lugar al cruce de información con otras disciplinas para satisfacer los RICC.

5.5.1. Planeamiento operacional

[5-76] La efectividad de las operaciones de CI depende, en gran medida, del planeamiento que precede a la operación. El planeamiento operacional incluye establecer las tareas de CI en la operación, la integración con unidades de combate, los canales de comunicación y el apoyo de CI para establecer el dominio de la información a través de la ejecución de sus tareas, buscando negar la información al adversario. Al comienzo del proceso de planeamiento, la CI dirige los esfuerzos para la recolección de información sobre las actividades de sabotaje, terrorismo, espionaje y subversión de la inteligencia de la amenaza.

CI	Contrainteligencia
OT	Organizaciones terroristas
PICC	Preparación de inteligencia del campo de combate
PMTD	Proceso militar para la toma de decisiones
PSPB	Proceso de selección y priorización de blancos
RICC	Requerimientos de información crítica del comandante

PSPB Proceso de selección y priorización de blancos	<p>[5-77] Esta información permite el desarrollo de actividades de CI para retener la iniciativa y evitar la sorpresa durante la ejecución de las operaciones militares. En el planeamiento previo al despliegue, se brinda la mayor cantidad posible de información sobre la amenaza de recolección de la información. Esto permite que se desarrolle una lista de objetivos de CI, la cual identifica las personas, las organizaciones y las instalaciones que deben aprovecharse, explotarse o protegerse, para proporcionar un dominio de la información de CI. La lista de blancos de CI ayudará en el PSPB para negar, mitigar o degradar la capacidad del adversario para recolectar información crítica de las operaciones. En este proceso se deberán desarrollar contramedidas, planes y, si es el caso, recomendar ataques a posiciones del enemigo, para lograr la explotación de la información de interés para la CI.</p>
CI Contrainteligencia	

5.5.2. Listas de blancos de CI

| Tabla 5-1 | Listas de blancos de CI

Personas	<ul style="list-style-type: none"> • Lista negra: Personal identificado como miembro de la amenaza, colaboradores, simpatizantes y recolectores de información. • Lista gris: Personal cuyas actitudes e inclinaciones no se encuentran plenamente establecidas pero que poseen información o habilidades de recolección de información que podrían ser objeto de estudio por parte de las propias tropas. • Lista blanca: Personal proclive al suministro de información, con actitudes de colaboración voluntaria.
Instalaciones	<ul style="list-style-type: none"> • Ocupadas por personal de la amenaza. • Objeto de acciones de inteligencia de la amenaza. • Centros de emisiones radiales clandestinas pertenecientes a la amenaza.
Organizaciones	<ul style="list-style-type: none"> • Organizaciones de inteligencia de la amenaza. • Organizaciones o grupos hostiles. • Organizaciones al margen de la ley.

[5-78] Las listas de blancos de CI establecen personas, instalaciones u organizaciones, que, debido a su actividad, su función o sus objetivos, manejan información considerada de interés para la CI y sobre los cuales se deben dirigir los esfuerzos de la disciplina.

5.5.2.1. Personas

[5-79] Personas que son consideradas una amenaza para la seguridad, cuyas intenciones se desconocen y que pueden ser o proveer ayuda a la inteligencia de la amenaza. Las personas se agrupan en tres categorías; para facilitar su identificación se emplea un código de color, que indica la categoría. Los colores actualmente en uso son: negro, gris y blanco.

5.5.2.1.1. *Lista negra*

[5-80] Se trata de un documento interno de CI que está amparado por la reserva legal establecida en la Ley Estatutaria 1621 de 2013, que se limita por el respeto a los derechos humanos y el DIH, y donde se relaciona a presuntos colaboradores, simpatizantes, agentes de inteligencia y otras personas reconocidas, sospechosas o que representan un potencial riesgo, dado que su presencia se interpreta como una amenaza a la seguridad de las propias tropas. La lista negra incluye:

- Personas con acusaciones conocidas o sospechosas de ser agentes de espionaje, hostiles, saboteadores, terroristas o individuos subversivos.
- Personas que sean agentes dobles o traficantes de información.
- Personas mencionadas en archivos de inteligencia y de CI como presuntamente pertenecientes a grupos armados organizados (guerrilleros, milicianos, extremistas, terroristas, entre otros).
- Conocidos o sospechosos de pertenecer a agencias adversarias cuya presencia en el AO representa un riesgo para la seguridad.
- Simpatizantes y colaboradores enemigos conocidos o sospechosos cuya presencia en el AO representa una amenaza para la seguridad.

CI | Contrainteligencia

DIH | Derecho internacional humanitario

AO | Área de operaciones

CI

Contrainteligencia

- Personal militar o civil de la inteligencia de la amenaza, ya identificados como tal, y que hayan participado en actividades de inteligencia, CI, seguridad o adoctrinamiento.
- Personas que hayan sido detenidas y tengan antecedentes de delitos o de actuaciones afines a la recolección de información.

5.5.2.1.2. Lista gris

[5-81] La lista gris contiene las identidades y las ubicaciones (actividad amparada por la Ley 1621, art. 5º, Principio de Necesidad) de las personas de quienes se sabe que poseen información o habilidades particulares de recolección de información o acceso a ella. Pueden ser individuos cuyas motivaciones requieren una mayor exploración antes de que puedan ser explotadas.

[5-82] Los ejemplos de personas que pueden incluirse en esta categoría son:

- Desertores potenciales o reales de la amenaza, pero cuya buena fe no ha sido establecida.
- Individuos que se han resistido, o se cree que han resistido, a la amenaza, y que pueden estar dispuestos a cooperar, pero cuya buena fe no se ha determinado.
- Fuentes o informantes cuya lealtad aún no ha sido comprobada.
- Desmovilizados o personal sometido a la justicia que fueron parte de OT o de organizaciones subversivas, pero de quienes aún no se ha logrado establecer una motivación para colaborar con agencias amigas.

OT

Organizaciones
terroristas

5.5.2.1.3. Lista blanca

[5-83] La lista blanca contiene las identidades y las ubicaciones de personas que son potencialmente proclives a proporcionar información de interés para la CI. Por lo general, están

de acuerdo con las políticas del gobierno colombiano o las de sus asociados, o que están favorablemente inclinadas hacia estas. Sus contribuciones se basan en una actitud voluntaria y de cooperación. Las decisiones de poner a individuos en la lista blanca pueden verse afectadas por la situación de combate y por necesidades de inteligencia. Los ejemplos de personas que pueden incluirse en esta categoría son:

- Personas que hayan ejercido un cargo político, y que en función de este hayan sido afines a los intereses de Colombia o de los asociados de la AU.
- Personal de inteligencia utilizado por agencias de inteligencia aliadas o propias.
- Informantes que han demostrado lealtad e información real durante un periodo considerable y demuestran un alto grado de confiabilidad.
- Personas que, por sus convicciones políticas, militares, sociales o religiosas, o por cualquiera otra que fuera su motivación, quieren colaborar con los fines o los objetivos de Colombia o los asociados de la AU.

AU | Acción unificada

5.5.2.2. Instalaciones

[5-84] Las instalaciones en la lista de blancos de CI son cualquier edificio, oficina o área que pueda contener información o material de interés para la CI o que pueda representar una amenaza para la seguridad nacional. Las instalaciones de interés de CI incluyen:

- Las que están o fueron ocupadas para realizar actividades de espionaje, sabotaje, agencias subversivas u organizaciones de la amenaza, incluidas cárceles y centros de detención.
- Aquellas ocupadas por la inteligencia enemiga, por la CI, por seguridad o por organizaciones armadas, incluidas las bases operativas y los sitios de entrenamiento.

CI | Contrainteligencia

- Centros de emisiones radiales clandestinas pertenecientes a la amenaza.
- Sedes administrativas donde se podría recolectar información.
- Servicios públicos y otras instalaciones de la infraestructura crítica que fuera necesario proteger para evitar su sabotaje.
- Instalaciones de producción, áreas de suministro y otras instalaciones que deben protegerse para evitar el apoyo a elementos subversivos o a agencias hostiles.

5.5.2.3. Organizaciones

CI | Contrainteligencia

[5-85] Cualquier grupo que sea considerado una amenaza potencial para la defensa nacional, la seguridad de la Fuerza o de una nación aliada debe ser objeto de actividades de CI. Estas actividades se desarrollarán dentro del marco de la Ley 1621 de 2013. Los grupos o las organizaciones que son de interés para la CI durante las operaciones incluyen:

AO | Área de operaciones

- Organizaciones de inteligencia de la amenaza.
- Partidos o grupos políticos nacionales y locales de los cuales se tiene conocimiento que apoyan algún tipo de organización armada o de milicias.
- Organizaciones de la amenaza que se valgan de estudiantes, policías, veteranos militares y excombatientes conocidos por ser hostiles para emplearlos en actividades de la inteligencia enemiga.
- Organizaciones o grupos hostiles cuyos objetivos son crear agitación entre la población civil en el AO.
- Organizaciones al margen de la ley, grupos armados organizados u organizaciones que los apoyan de cualquier forma.



LA CAPACIDAD DE ANÁLISIS, UNA VIRTUD INDISPENSABLE DE LOS HOMBRES DE INTELIGENCIA

En 1997, agentes de CI obtuvieron información sobre la existencia de una bodega ubicada al sur de la ciudad de Bogotá, donde, según se pudo establecer inicialmente, un grupo perteneciente a la guerrilla del ELN estaría fabricando de manera clandestina armas no convencionales y artefactos explosivos improvisados (AEI). Sin embargo, la información recolectada hasta el momento no era lo suficientemente específica para iniciar una operación de CI, ya que no se había podido localizar la ubicación exacta de la bodega y los indicios no eran concretos.

Para esa época, la inteligencia colombiana no había adoptado ninguna metodología de análisis estructural. No obstante, el hecho de no obtener resultados por medios humanos obligó a la CI a desarrollar un análisis empírico sobre la información recolectada; así se logró establecer nuevos indicios, que sirvieron para reorientar el esfuerzo de búsqueda de los agentes que se encontraban desarrollando actividades encubierta, lo que, finalmente, permitió dar con la ubicación de la fábrica, donde se realizó la captura del personal encargado de la producción, así como la incautación de diferentes clases de herramientas hechizadas que eran empleadas para la fabricación de lanzacohetes, "tatuco" y cilindros, entre otros.

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

CAPÍTULO 6

SERVICIOS TÉCNICOS DE CONTRAINTELIGENCIA

“(...) Esto es algo imperativo para los guerreros; ignorar la maestría de las armas y la comprensión de las ventajas específicas de cada una de ellas sería indicar una falta de cultura de un miembro de una casa guerrera”.

Miyamoto Musashi



[6-1] El desarrollo de las averiguaciones se ha mejorado de manera significativa debido al uso de tecnología tradicional y emergente, diseñada para simplificar y reducir el tiempo necesario para completar ciertas tareas de CI. Simultáneamente, esto garantiza que toda la información obtenida, sin importar si se la considera insignificante o irrelevante, sea evaluada de manera eficaz. Las unidades de CI cuentan con personal capacitado en los servicios técnicos de CI para proporcionar los apoyos necesarios.

6.1. GENERALIDADES

[6-2] Los servicios técnicos de CI son actividades que se llevan a cabo para orientar y apoyar el esfuerzo de recolección de información durante el desarrollo de averiguaciones o la ejecución de operaciones de CI en apoyo a las unidades del Ejército y todo el rango de operaciones militares (ROM). Estas actividades emplean herramientas o equipos técnicos que realizan tareas específicas de acuerdo con el tipo de información y la fuente de la cual se obtuvo dicha información.

CI | Contrainteligencia

[6-3] Generalmente, estos servicios se llevan a cabo cuando se obtienen indicios o pruebas que deban ser procesados o analizados y cuando se requieran medios técnicos para comprobar la veracidad de la información recolectada, por lo cual los mencionados servicios se constituyen en un apoyo a las averiguaciones y se desarrollan como complemento a las tareas de recolección de información que realiza la CI.

[6-4] Las unidades que requieran el empleo de uno o varios servicios técnicos, deberán solicitar el apoyo al Comando de Contrainteligencia (CACIM), el cual se encargará de tramitar las solicitudes y ordenar a la unidad correspondiente, suministrar el apoyo requerido, siempre y cuando se establezca que su propósito y su objetivo corresponden a los fines y límites de la inteligencia y CI.

FCG | Función de conducción de la guerra

[6-5] Algunos servicios técnicos desarrollan actividades propias de otras disciplinas de las FCG Inteligencia e incluso pueden ser empleados con el mismo nombre. Sin embargo, el

presente capítulo define y establece únicamente las tareas que se ejecutan dentro de la disciplina de CI y explica cómo deben ser implementadas para actividades y operaciones de CI.

[6-6] Los servicios técnicos son ejecutados por agentes de CI capacitados y certificados para tal fin, y quienes contribuyen significativamente a las actividades de CI. Estos proporcionan al comandante información oportuna y objetiva para el PMTD. Una unidad de CI que esté desarrollando una operación puede solicitar el apoyo de uno o varios servicios técnicos. Dichos servicios son:

- Inteligencia de fuentes abiertas (OSINT, por su sigla en inglés).
- Contramedidas de vigilancia electrónica.
- Identificación mediante características biométricas
- Pruebas técnicas psicofisiológicas de veracidad.
- Informática forense.

PMTD	Proceso militar para la toma de decisiones
CI	Contrainteligencia

6.2. INTELIGENCIA DE FUENTES ABIERTAS (OSINT)

[6-7] La *inteligencia de fuentes abiertas* es una disciplina complementaria de la inteligencia producida a partir de información públicamente disponible que es recolectada, explotada y difundida oportunamente a una audiencia apropiada, con el fin de atender un requerimiento específico de inteligencia (MFRE 2-0). Las actividades de OSINT que se llevan a cabo dentro de la disciplina de CI tienen por objeto complementar los productos de CI, dando un valor agregado a partir de información que procede de fuentes públicamente disponibles, que contribuyan a responder a los vacíos de información dentro del desarrollo de las actividades de CI.

OSINT	Inteligencia de fuentes abiertas
-------	----------------------------------

[6-8] En este sentido el ámbito de la obtención, la gestión, la integración, el análisis y la difusión de información abierta es propicio para aplicar la tecnología disponible y las capacidades

OSINT

Inteligencia de fuentes abiertas

CI

Contrainteligencia

intelectuales que a la postre repercutirán en la calidad de los productos ofrecidos por los analistas de CI.

[6-9] El manejo de fuentes abiertas para producir inteligencia en apoyo de las decisiones es de largo alcance, aunque estas deben considerarse como un medio complementario. En tal escenario, la diferencia entre un producto de OSINT de calidad y otro de menor categoría recae en el analista antes que en la cantidad y la calidad de la información disponible, y para ello, no es necesario que la información sea secreta. El cómo y el cuándo utilizar los productos de OSINT dependerá del analista y del responsable de la toma de decisiones.

[6-10] Los datos de fuentes abiertas están comprendidos, entre otros, por la prensa, la radio, discursos, redes sociales, información disponible en internet y demás modalidades que vengan de fuentes primarias. También pueden ser fotografías, videos e imágenes satelitales comerciales; llegan incluso a cartografías disponibles públicamente. La información de fuentes abiertas es el resultado de correlacionar los datos sobre un mismo tema siguiendo un proceso de validación donde entran en juego factores de selección, relación, análisis y difusión. La OSINT es la transformación que sufre la información recolectada, valorada, verificada y difundida a un destinatario seleccionado para resolver un vacío o una duda.

6.2.1. Empleo de OSINT en los niveles de la guerra

[6-11] La CI emplea OSINT en el nivel estratégico de manera preventiva o anticipativa, por lo que esta se convierte en una herramienta valiosa para determinar indicadores de alerta o precaución ante la posibilidad de un incidente. Es la manera más sencilla y económica para determinar la estabilidad o inestabilidad de una zona de interés, sin poner en riesgo la integridad física de agentes. En este nivel, la OSINT también aporta a los sistemas de inteligencia del orden nacional la secuencia histórica de acontecimientos de interés para una crisis y también puede llegar a analizar la opinión pública. En este nivel, el esfuerzo de búsqueda de OSINT se encuentra direccionado hacia la recolección de información de servicios

de inteligencia y seguridad extranjeros y la identificación y el seguimiento de indicios y pruebas relacionadas con organizaciones terroristas internacionales.

[6-12] En el nivel operacional, este servicio técnico se emplea para recolectar y analizar información relacionada con aspectos políticos, geográficos, biográficos, económicos y tecnológicos que puedan suministrar información que contribuya a la identificación de objetivos de interés para las operaciones de CI y categorizar riesgos y amenazas basados en las tendencias que arrojan las herramientas automatizadas.

CI | Contra Inteligencia

[6-13] En el nivel táctico, la OSINT se emplea para hacer seguimiento a actividades específicas de un objetivo de CI. En este nivel se emplean diferentes técnicas para obtener información de gran cantidad de medios disponibles (físicos y digitales) que puedan suministrar datos relacionados con publicaciones, comentarios, búsquedas en internet, gustos, preferencias, actividades diarias y acciones particulares de un objetivo reconocido durante el transcurso de una operación o una averiguación de CI. De igual manera, este servicio técnico se utiliza para proporcionar acceso a una gran variedad de información sobre infraestructura, asuntos locales, terreno o población civil que contribuya a configurar un ambiente operacional.

OSINT | Inteligencia de fuentes abiertas

6.2.2. Ventajas de la OSINT

[6-14] En resumen, las ventajas de la OSINT sobre las demás disciplinas de la inteligencia incluyen la rapidez en la consecución de la información relacionada con un asunto específico y el hecho de ser más económica y no representar riesgos jurídicos al emplearla. Además, el uso y el consumo de la información se proporcionan en cualquier formato, provee técnicas de recuperación de información, automatización de alertas, novedades de temas específicos, presentación de resultados mediante gráficas y otras muchas ventajas, que se añaden conforme vaya avanzando la tecnología y se incrementen las fuentes de información públicamente disponibles. Estas ventajas son aprovechadas por la CI para suministrar

información en tiempo real de las amenazas que puedan llevar a cabo acciones de espionaje, sabotaje, subversión o terrorismo.

OSINT

Inteligencia de fuentes abiertas

6.2.3. Desventajas de la OSINT

[6-15] Al enfrentarse a un gran volumen de información públicamente disponible, los analistas, requieren plataformas y centros especialmente organizados para realizar OSINT; esto, dada la dificultad de determinar la fuente exacta de algunas informaciones y la de estimar la veracidad de estas, lo cual implica el consumo valioso del tiempo de trabajo. La baja importancia que algunos servicios de inteligencia le dan a la OSINT, la posiciona muy mal dentro de los criterios orientadores para la toma de decisiones; sin embargo, se requiere que esta no trabaje de manera aislada, sino, por el contrario, que se integre a las otras actividades de CI, para responder a los interrogantes de información y que, de esta forma, los comandantes o los tomadores de decisión a todo nivel consideren y evalúen la inteligencia producida por esta disciplina. La incompatibilidad entre los diferentes formatos, fuentes y bases de datos requiere el uso de tecnología de Big Data, para precisar el uso de herramientas multilenguaje.

CI

Contrainteligencia

6.2.4. Explotación de la OSINT en apoyo a las actividades de contrainteligencia

[6-16] Para la CI, el punto de partida de la OSINT comienza cuando se hace una revisión preliminar del tema por tratar antes de iniciar la recolección de información. De la revisión debe salir una serie de fundamentos que serán empleados en la búsqueda para llenar los vacíos existentes y de esto, a su vez, se desprenderán las fuentes que se vayan a utilizar para la recolección de información. Para la explotación de la OSINT se consideran cuatro pasos:

- **Paso 1. Seguridad:** las actividades de OSINT deben ser ejecutadas teniendo como base primordial todas las

medidas de seguridad requeridas para negar la recolección de información propia por parte de la amenaza, y evitar así la presencia de indicadores de labores de OSINT durante los pasos subsiguientes. El principio de la seguridad se tendrá que ver representado en el anonimato de red y el cifrado de tipo militar sobre toda la información recolectada y procesada. Además de eso, se debe contar con todos los elementos de seguridad de información y seguridad informática estándar en cualquier sistema de información.

- **Paso 2. Identificación:** para generar productos de OSINT en apoyo de las averiguaciones y las actividades de CI, es necesario que el analista desarrolle habilidades técnicas y un nivel avanzado de experticia, que se originan en el conocimiento de las fuentes primarias y secundarias de información de fuentes abiertas disponibles. La base primaria de la explotación de OSINT es esencialmente la identificación de todas las fuentes importantes de OSINT y saber cómo buscar. En resumen, el conocimiento eficaz sobre el tratamiento de las fuentes de OSINT es el punto esencial para proporcionar productos de OSINT de calidad.
- **Paso 3. Segregación y filtrado:** los resultados obtenidos en las búsquedas realizadas no garantizan por sí solos que se vaya a obtener un producto de OSINT útil para los objetivos de CI. Estos resultados se deben optimizar mediante procesos de selección, integración y valoración que hacen del producto de OSINT un recurso valioso en términos de exhaustividad y de pertinencia documental. El resultado debe representar la esencia del conocimiento que proporciona la búsqueda, la selección, la integración, la valoración y los análisis. El producto de OSINT es la síntesis objetiva de la integración de fuentes, formatos y análisis aplicados a un fin específico.
- **Paso 4. Difusión:** los agentes que sean destinados para suministrar el apoyo de este servicio técnico, deberán entregar en tiempo real los productos de OSINT a la unidad

OSINT | Inteligencia de fuentes abiertas

CI | Contrainteligencia

que solicitó el apoyo, de manera que la información pueda ser empleada oportunamente dentro del desarrollo de la operación; sin embargo, el agente deberá también elaborar un informe de recolección de información dirigido a la unidad de la cual es orgánico, en el que se relacionen las actividades realizadas durante el apoyo suministrado a la operación de CI. Las unidades receptoras deberán emplear estos productos únicamente para los fines establecidos en el artículo 4 de la Ley 1621 de 2013.

[6-17] Para la CI, la recolección y el procesamiento de información de fuentes abiertas es aplicable a determinados tipos de OSINT, los cuales se dividen en:

OSINT | Inteligencia de fuentes abiertas

CI | Contrainteligencia

- **OSINT básica:** es general, permanente en el tiempo y utilizada como banco de datos, podrá comprender ficheros biográficos, características generales de un país o zona, persona, organización o evento relevante.
- **OSINT actual:** con la que se mantiene actualizada la OSINT básica. Abarca información de actualidad sobre un asunto, un país o una situación específica.
- **OSINT para objetivos de CI:** dirigida a identificar operaciones, enemigos o adversarios en una situación concreta. Esta determina, en síntesis, el curso de adopción más probable del enemigo.

6.3. CONTRAMEDIDAS DE VIGILANCIA ELECTRÓNICA

[6-18] Las contramedidas de vigilancia electrónica son consideradas un servicio técnico de CI porque requieren el empleo de equipos electrónicos para contrarrestar las acciones de espionaje por parte de la amenaza. La CI dispone de este servicio para suministrar apoyo a todas las unidades del Ejército que lo requieran. A diferencia de los demás servicios técnicos, este se desenvuelve en un contexto mucho más amplio, porque es empleado tanto en actividades operacionales como administrativas y no se limita únicamente a apoyar las operaciones de CI.

[6-19] La **vigilancia electrónica** es el **uso de dispositivos electrónicos para controlar o monitorear actividades, comunicaciones, sonidos o impulsos electrónicos**. Las contramedidas de vigilancia electrónica buscan contrarrestar la vigilancia electrónica desarrollada por una amenaza, un enemigo o un adversario. Las actividades de contramedidas de vigilancia electrónica son llevadas a cabo para apoyar una operación de CI, proteger un área determinada donde se lleven a cabo reuniones o actividades que traten temas operacionales, de inteligencia y de CI o cualquier otro tipo de carácter sensible y crítico. También se empleará en las áreas determinadas por OPSEC o seguridad militar, de acuerdo con la evaluación de amenazas y vulnerabilidades.

CI	Contrainteligencia
OPSEC	Seguridad de las operaciones

[6-20] Las actividades de contramedidas de vigilancia electrónica contribuyen a la superioridad en la información para disminuir o neutralizar la recolección de información de las organizaciones terroristas, el crimen organizado y las amenazas emergentes, que pretendan acceder a información reservada o clasificada del Ejército. Estas actividades incluyen la evaluación y el control de las emanaciones electromagnéticas, lo que se refiere a la transmisión de información mediante ondas electromagnéticas que hacen posible la comunicación entre dos dispositivos electrónicos o la transferencia de datos entre estos. En sentido general, este servicio técnico se emplea para evitar el espionaje electrónico en el ámbito de la información, en donde se ponga el riesgo el secreto de las operaciones y las actividades militares.

[6-21] Estas contramedidas están diseñadas para contrarrestar el esfuerzo de recolección de información de la inteligencia extranjera o de cualquier otro tipo amenaza que actúe mediante la inserción de dispositivos encubiertos o clandestinos en una instalación, la modificación de equipos existentes dentro de un área crítica u otra catalogada como actividad de vigilancia electrónica. En su mayor parte, la inteligencia obtenida del uso de la vigilancia electrónica será considerada como información precisa, pues las personas no son conscientes de que están siendo monitoreadas.

[6-22] La amenaza utiliza todos los medios disponibles para recolectar información reservada o clasificada. Una forma de hacer esto es mediante el uso de dispositivos técnicos de control, al mismo tiempo que través de los fallos de seguridad provocados circunstancial o intencionalmente en equipos electrónicos utilizados en las instalaciones militares. La amenaza explota estas debilidades para obtener información de las conversaciones confidenciales o clasificadas y conocer detalles del planeamiento de las unidades. Para la amenaza, este tipo de información puede ser de gran importancia ya que le permite conocer o anticipar las intenciones futuras de las propias tropas. Cabe destacar que la vigilancia electrónica no solo se lleva a cabo mediante dispositivos de audio, sino que incluye señales y transmisión de video. La amenaza instala los dispositivos de vigilancia en lugares donde el personal militar no pueda detectarlos sin el empleo de equipos especializados y de personal capacitado.

[6-23] El propósito principal de las contramedidas de vigilancia electrónica es localizar y neutralizar los dispositivos técnicos de control que hayan sido instalados en áreas restringidas del Ejército, e incluye todas las medidas adoptadas para reducir el riesgo de vigilancia electrónica. El propósito secundario es proporcionar a los comandantes y a los jefes de dependencias una evaluación completa de las condiciones de seguridad electrónica y física de sus instalaciones, y conscientizar al personal con respecto a las amenazas de vigilancia electrónica.

CI

Contrainteligencia

[6-24] Las contramedidas incluyen cinco actividades de CI separadas, y cada una, con una influencia directa en el desarrollo de estas:

- **Detección:** estas actividades son diseñadas para detectar la presencia de dispositivos técnicos de vigilancia, riesgos de seguridad técnica, física o deficiencias de seguridad que posibiliten la extracción de información reservada o clasificada por parte de la amenaza.
- **Anulación:** incluye tanto medidas para negar las actividades de los dispositivos detectados, como las acciones

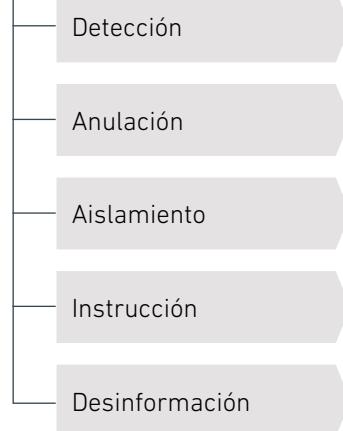
para neutralizar su funcionamiento. Un ejemplo de anulación es la insonorización. Sin embargo, la insonorización, que cubre solo una parte de un área determinada, no es muy útil ya que el uso de cables excesivos podría ser utilizado como un medio para el transporte de datos dentro del área protegida. La anulación también se refiere a las medidas adoptadas para que la instalación de los sistemas técnicos de control por parte de la amenaza no sea posible; esto incluye medidas de seguridad física.

- **Aislamiento:** se refiere a la adecuación de áreas restringidas para el manejo de información crítica, en donde le sea negado el acceso a terceros o a cualquier persona que no cuente con la autorización del comandante. El aislamiento puede implicar la designación de un área especial más pequeña con barreras de seguridad física y otras medidas apropiadas. El aislamiento podrá emplearse en un edificio completo, si es necesario.
- **Instrucción:** el personal militar debe conocer la amenaza de vigilancia electrónica y tener claras sus responsabilidades y sus compromisos antes de que un dispositivo de vigilancia electrónica sea detectado o se sospeche su existencia. Además, el personal deberá encontrarse alerta ante lo que esté sucediendo en y alrededor de su área, sobre todo durante la construcción, la renovación o la instalación de nuevos equipos.
- **Desinformación:** cuando el dispositivo de vigilancia electrónica sea descubierto, la CI puede enviar mensajes falsos con el fin de desinformar y engañar sobre la recolección de información del enemigo.

[6-25] Las contramedidas electrónicas se ejecutarán a través de técnicas de seguridad militar establecidas en el manual dispuesto para tal fin.

[6-26] Este servicio técnico desarrolla tres actividades prioritarias para contrarrestar el accionar de la amenaza sobre la información de la unidad apoyada. Estas actividades facilitan el planeamiento y la ejecución en todo el rango de las operaciones militares.

ACTIVIDADES DE CONTRAMEDIDAS



CI

Contrainteligencia

| **Tabla 6-1** | Actividades prioritarias de las contramedidas electrónicas

Examen de contramedidas de vigilancia electrónica	<ul style="list-style-type: none"> • Detecta elementos de vigilancia electrónica. • Analiza debilidades de seguridad física y técnica.
Inspección de contramedidas de vigilancia electrónica	<ul style="list-style-type: none"> • Actividad posterior al examen de vigilancia electrónica. • Se realiza por aumento de indicios de amenaza o por sospecha de penetración electrónica.
Apoyo de contramedidas de vigilancia electrónica previas a la construcción	<ul style="list-style-type: none"> • Estudio preliminar a la construcción de instalaciones militares (solución de requerimientos de seguridad).

6.3.1. Examen de contramedidas de vigilancia electrónica

[6-27] Se trata de un examen desarrollado de forma electrónica, física y visual con un carácter detallado y completo, y hecho para detectar los elementos clandestinos de vigilancia que puedan haber sido implantados en una instalación militar. Durante el desarrollo de este examen es posible identificar las debilidades de seguridad física y técnica, que podrían ser explotadas por la amenaza, los enemigos o los adversarios.

6.3.2. Inspección de contramedidas de vigilancia electrónica

[6-28] Normalmente, una vez un examen de contramedidas de vigilancia electrónica se ha llevado a cabo, este no se repetirá; sin embargo, si el personal de CI encuentra numerosas deficiencias técnicas o físicas durante el examen, puede solicitar una inspección de contramedidas de vigilancia electrónica en una fecha posterior. También se podrá programar y realizar una inspección si se ha detectado un aumento de indicios de la amenaza de vigilancia electrónica en una instalación o si existe alguna sospecha de que se encuentra en proceso una penetración técnica en el área.

VIGILANCIA ELECTRÓNICA

Uso de dispositivos electrónicos para controlar o monitorear actividades, comunicaciones, sonidos o impulsos electrónicos (MCE 2-22.1).

CARACTERÍSTICAS BIOMÉTRICAS

Rasgos biológicos y de comportamiento distintivos de una persona que se pueden utilizar para el reconocimiento automatizado (MCE 2-22.1).

INFORMÁTICA FORENSE

Aplicación de técnicas especializadas para obtener, preservar o restablecer datos que han sido procesados digitalmente y almacenados en un dispositivo electrónico (MCE 2-22.1).

6.3.3. Apoyo de contramedidas de vigilancia electrónica previas a la construcción

[6-29] El apoyo realizado previo a la construcción o la adecuación de una instalación militar tiene como objetivo garantizar que un edificio o área se construirán con los estándares de seguridad exigidos para las actividades que se van a realizar en su interior. Al igual que con otras áreas técnicas, es mucho menos costoso y más eficaz construir con base en una buena seguridad desde las etapas iniciales de un nuevo proyecto; además, hacerlo disminuye gastos de modificaciones o reformas posteriores al terminado de la obra.

[6-30] Las actividades de contramedidas de vigilancia electrónica previas a la construcción de unidades militares se llevarán a cabo tomando en cuenta que:

- Las solicitudes deberán ser presentadas con antelación a la fecha en que se requiere la ejecución de la actividad; en caso de presentarse requerimientos de urgencia dado el riesgo o la amenaza, deberán soportarse y emitirse de igual forma las solicitudes pertinentes a la ejecución del apoyo.
- La divulgación de información relacionada con las actividades de un servicio de contramedidas de vigilancia electrónica es una violación grave de seguridad con consecuencias potencialmente negativas para la seguridad nacional. No se debe poner en peligro la divulgación del servicio a cualquier persona; especialmente, una dentro de la instalación, ya que si un dispositivo de escucha es instalado en la zona, puede alertar a las personas que están llevando a cabo la vigilancia, y les permitirá eliminar o desactivar sus dispositivos. Cuando se desactivan, tales dispositivos son extremadamente difíciles de localizar y buscarlos puede requerir la aplicación de técnicas de búsqueda destructivas.
- Si durante las labores de construcción se presenta un evento (accidentes o cortocircuitos, entre otros) que comprometa al personal de CI, el responsable de la misión deberá poner fin a las actividades e informar a la unidad

que solicitó el apoyo sobre las circunstancias asociadas al riesgo; y no se reprogramarán actividades hasta que la causa y el efecto del evento o incidente ocurrido hayan sido evaluadas por el personal de CI.

CI | Contrainteligencia

[6-31] Una vez completado un examen o una inspección de contramedidas de vigilancia electrónica, el objetivo debe ser que el solicitante tenga la seguridad de que la zona estudiada se encuentra libre de dispositivos técnicos de control y de que sus activos no estarán en riesgo. El jefe de la misión informará al solicitante:

- Sobre todas las vulnerabilidades de seguridad técnicas y físicas encontradas con las acciones correctivas recomendadas en cada caso.
- Que es imposible dar una garantía positiva y absoluta de que no existen dispositivos en el área estudiada, pero el nivel de riesgo posterior al desarrollo de la actividad disminuye representativamente.
- Que la seguridad será vulnerada si no se aplican medidas para restringir el acceso a la zona verificada a personas que carezcan de la corroboración de su credibilidad y su confiabilidad o que no cuenten con el nivel de acceso requerido.

[6-32] Las actividades de contramedidas de vigilancia electrónica no serán efectivas si no se realiza un control constante del área inspeccionada, de forma continua y eficaz, ya que esto permitiría reparaciones o modificaciones por parte de personas que carecen de la debida autorización de seguridad o que no se encuentren bajo la supervisión de personal idóneo. De igual manera, el resultado de la aplicación de contramedidas electrónicas se verá afectado por la introducción de nuevos muebles o equipos sin una inspección minuciosa a cargo de personal experto.

[6-33] Toda la información relativa al descubrimiento de un dispositivo de vigilancia electrónica será procesada contemplando las medidas para preservar el secreto. Inmediatamente se iniciarán las averiguaciones pertinentes con apoyo de todos los servicios técnicos a fin de identificar las

personas responsables de la vigilancia electrónica o establecer el origen de esta.

6.4. IDENTIFICACIÓN MEDIANTE CARACTERÍSTICAS BIOMÉTRICAS

[6-34] Las **características biométricas** son **rasgos biológicos y de comportamiento distintivos de una persona que se pueden utilizar para el reconocimiento automatizado**. La identificación mediante características biométricas es una actividad que de forma automatizada permite el reconocimiento de una persona con base en una característica fisiológica o del comportamiento.



NOTA

MASINT

Inteligencia de medidas y huellas distintivas

La ejecución de este servicio técnico puede requerir el empleo de una o varias técnicas de MASINT.

[6-35] Entre las características fisiológicas o de comportamiento distintivas se encuentran la cara, las huellas dactilares, la geometría de las manos, la escritura, el iris, la retina y la voz. Las tecnologías biométricas se están convirtiendo en la base de una amplia gama de formas de identificación altamente seguras y soluciones de verificación personal. A medida que el nivel de las brechas de seguridad y de fraude va en aumento, la necesidad de identificación y de la tecnología de verificación biométrica personal es cada vez más evidente.

CI

Contrainteligencia

[6-36] Con una perspectiva de CI, la biometría proporciona una herramienta que se emplea para determinar a personas durante el desarrollo de operaciones y detección a través de la información obtenida por bases de datos. La CI también podrá utilizar este servicio técnico para obtener huellas digitales después de una acción hostil, que permitan la identificación del fabricante de artefactos explosivos o a los ejecutantes de otras actividades irregulares.

[6-37] Se requieren herramientas biométricas para la identificación de características sobre bases de datos y para realizar

controles de personas durante las operaciones de CI, de manera que se pueda contribuir a la configuración de un análisis preciso. Las características biométricas incorporan varios criterios fisiológicos, como el ADN (ácido desoxirribonucleico), el reconocimiento de voz, el reconocimiento de iris, los datos de las huellas dactilares y las características faciales, para mejorar significativamente las operaciones y el análisis de CI.

CI | Contrainteligencia

[6-38] Las bases de datos de características biométricas aumentarán la capacidad de identificar, rastrear y validar las fuentes de inteligencia a través de la identificación fisiológica y de los indicios de engaño. El equipo de identificación biométrica deberá contar con:

- Escáner de huellas digitales, escáner de iris y cámaras digitales para la entrada de datos.
- *Software* de reconocimiento para la identificación basada en criterios fisiológicos.
- *Software* de base de datos para archivar información de reconocimiento y comparación de identidad.
- *Software* de análisis y reconocimiento de voz.

6.5. APOYO DE PRUEBAS TÉCNICAS PSICOFISIOLÓGICAS DE VERACIDAD

[6-39] Las pruebas técnicas psicofisiológicas de veracidad se describen como el empleo de instrumentos técnicos o tecnologías emergentes, capaces de registrar las alteraciones psicofisiológicas en una persona, y que permiten, ante la generación de un estímulo (un enunciado o una pregunta), determinar los cambios involuntarios presentados en el cuerpo, asociados a conductas de engaño, los cuales podrán ser analizados y evaluados para emitir un diagnóstico o un resultado.

[6-40] Bajo ese entendido las tecnologías emergentes para pruebas técnicas psicofisiológicas de veracidad son las innovaciones científicas que pueden crear una nueva industria o transformar una existente, y las cuales podrán emplearse en

este caso de manera independiente, como complemento o reemplazo de una existente en materia de medición de reacciones psicofisiológicas asociadas a conductas de engaño, en el desarrollo de pruebas técnicas psicofisiológicas de veracidad.

6.5.1. Exámenes psicofisiológicos de polígrafo

[6-41] La CI en la actualidad cuenta con el polígrafo como un instrumento de diagnóstico empleado en el examen psicofisiológico de polígrafo o *Psychophysiological detection of deception* (PDD, por su sigla en inglés), que es capaz de monitorear, grabar y medir simultáneamente, como mínimo, actividad respiratoria, electrodérmica y cardiovascular, como respuesta a estímulos auditivos o visuales.

PDD

Psychophysiological
detection of deception

[6-42] A través del polígrafo se desarrolla el examen PDD, el cual es un proceso que abarca todas las actividades que tienen lugar entre un examinador PDD y un examinado, en una serie específica de interacciones.

[6-43] Las interacciones del PDD influyen la entrevista previa al examen, así como el uso del instrumento de polígrafo para recoger los datos fisiológicos de la persona examinada mediante la presentación de una serie de preguntas, la fase de análisis de datos de prueba y la fase posterior a la prueba.

- **Pretest:** fase preliminar de la prueba poligráfica que busca preparar psicológicamente al individuo para la evaluación. De este modo se obtiene la información que el examinado está dispuesto a suministrar. El pretest inicia desde el momento en que el poligrafista hace el contacto inicial con el examinado, y es cuando se hace el acondicionamiento mental del sujeto.
- **Test:** es la fase del examen poligráfico en la cual se grafican, se califican y se interpretan las gráficas poligráficas.
- **Posttest:** fase del examen poligráfico en la que el examinado tiene la oportunidad razonable de explicar las reacciones fisiológicas que presentó frente a las preguntas

hechas en los registros, mediante el desarrollo de la segunda fase de la entrevista poligráfica.

[6-44] Existen cuatro tipos de exámenes poligráficos, los cuales tienen finalidades específicas para cumplir los requerimientos de información del comandante: vinculación, desempeño, diagnóstico y de apoyo.

[6-45] El examen psicofisiológico de polígrafo es una de las pruebas técnicas psicofisiológicas de veracidad, cuyo desarrollo tiene su soporte jurídico en el marco de los estudios de credibilidad y confiabilidad, definidos en el título 3, capítulo 10, del Decreto 1070 de 2015.

[6-46] Las pruebas técnicas psicofisiológicas de veracidad se llevan a cabo como parte del estudio de credibilidad y confiabilidad o de manera independiente con el fin de contribuir al desarrollo de averiguaciones, operaciones de CI y operaciones militares a todo nivel.

CI

Contrainteligencia

[6-47] El examen psicofisiológico del polígrafo se podrá emplear siempre y cuando no se hayan iniciado formalmente investigaciones penales, disciplinarias, fiscales o administrativas. Cualquier requerimiento relacionado con el desarrollo de exámenes psicofisiológicos de polígrafo deberá tener el aval del comité de revisión de requerimientos de la unidad competente en dicha actividad.

[6-48] Este examen y su resultado se presentan como un criterio orientador que deberá ser corroborado a través de otras labores de recolección de información; de esa forma, se deben presentar los resultados y la información pertinente al caso, de manera conjunta con otras pruebas o exámenes técnicos que hacen parte del estudio de credibilidad y confiabilidad, para ser analizada, y así:

- Determinar la confiabilidad y credibilidad de los integrantes del Ejército Nacional y de otro personal que requiera ser evaluado de acuerdo con las necesidades de la fuerza, a fin de mantener altos estándares en materia de seguridad e integridad institucional.

- Determinar y elegir al personal para el desarrollo de actividades propias de inteligencia y de Cl.
- Determinar la veracidad de las informaciones que suministra una fuente de inteligencia o de Cl.

[6-49] La práctica del examen psicofisiológico de polígrafo será grabada en audio y video con fines de control de calidad y como garantía de los derechos fundamentales del examinado, de igual forma, para el desarrollo del examen es requisito indispensable el consentimiento de la persona a quien se va a examinar, y la cual, de manera libre, previa, informada y voluntaria, mediante documento escrito, accederá a la realización del examen. La manifestación de voluntad del evaluado prevalecerá por encima de las órdenes impartidas por un comandante en cualquier nivel del mando, y en caso de desistimiento por parte del examinado, este deberá informarlo por escrito en el documento destinado para tal fin.

[6-50] Para la preparación del examen el agente de Cl que posee la información inicial del caso por evaluar (en caso de que exista), deberá informarla previamente con el fin de desarrollar el adecuado proceso de construcción de preguntas y orientar el esfuerzo de búsqueda de información durante la entrevista poligráfica.

6.6. INFORMÁTICA FORENSE

[6-51] **Informática forense** se define como la **aplicación de técnicas especializadas para obtener, preservar o restablecer datos que han sido procesados digitalmente y almacenados en un dispositivo electrónico**.

[6-52] La informática forense empleada como un servicio técnico de Cl, independiente o en apoyo de las competencias propias de los investigadores judiciales, se lleva a cabo para:

- Identificar y recuperar datos relacionados con incidentes contra los activos informáticos del Ejército.

- Restaurar datos de dispositivos electrónicos que hayan sido obtenidos en el desarrollo de una operación de CI.
- Verificar y analizar registros digitales de dispositivos electrónicos involucrados en una averiguación de CI.
- Establecer cursos de acción para el desarrollo de averiguaciones de CI.

CI

Contrainteligencia

[6-53] Cada unidad de CI es responsable de identificar la necesidad del apoyo de informática forense requerido para sus averiguaciones o sus operaciones. Los análisis de informática forense aplican un proceso metódico que, dependiendo del tamaño y de la complejidad de los datos de medios digitales, puede llevar una cantidad significativa de tiempo para completarse. El proceso de las actividades de informática forense no puede apresurarse, y, por lo tanto, en muchas ocasiones es necesario restablecer la línea de tiempo para completar el proceso y, de esta manera, obtener la información requerida por la averiguación de CI.

6.6.1. Procedimiento para el manejo de datos digitales

[6-54] El procesamiento y el análisis de datos de medios digitales son tareas dispendiosas y lentas que requieren equipamiento tecnológico especializado y deben ser llevadas a cabo por personal de CI entrenado y capacitado en informática forense. Una falla en el adecuado procesamiento de los datos obtenidos o recuperados podría alterar la información, y hacer que esta pierda credibilidad para el desarrollo de futuras operaciones o averiguaciones de CI.



| Figura 6-1 | Procedimiento para el manejo de datos digitales

[6-55] El manejo de datos digitales es un procedimiento que consta de cuatro pasos específicos, estos son:

- **Paso 1. Identificación:** en este paso se obtiene información detallada de los datos digitales, que permita identificar a los posibles responsables, las causas y los elementos vinculados a un incidente de información, así como su estado actual, su ubicación, sus características y sus antecedentes, con el fin de establecer las herramientas y los recursos que se utilizarán en los siguientes pasos del procedimiento.
- **Paso 2. Recolección:** este paso consiste en determinar la metodología que se utilizará para la adquisición de muestras dependiendo del tipo de datos digitales que se requieran, con el fin de preservar las muestras que puedan ser volátiles (datos alojados en memoria RAM) y, posteriormente las no volátiles (datos alojados en dispositivos de almacenamiento).
- **Paso 3. Adquisición:** en este paso se realiza la extracción de imágenes forenses (únicamente bajo el principio de necesidad, de conformidad con el artículo 5 de la Ley 1621) a todos los dispositivos electrónicos que estén

vinculados en una averiguación de CI relacionada con la materialización de un incidente de información. Se deben utilizar siempre copias *bite a bite* para evitar que se modifique cualquier tipo de dato: de esta manera, es posible recuperar archivos borrados o particiones ocultas y obtener así una imagen de igual tamaño al disco procesado. Rotuladas con fecha, hora y huso horario, las muestras deberán ser aisladas de manera que no permitan el deterioro ni el contacto con el entorno. De igual forma, se debe obtener un registro fotográfico de los dispositivos electrónicos de los cuales se trajeron muestras, con el fin de registrar el estado de los elementos.

CI

Contrainteligencia

- **Paso 4. Preservación:** este paso consiste en proteger o asegurar la información obtenida en el paso anterior, para así evitar cualquier tipo de modificación, pérdida o destrucción de los datos recolectados. Por tal motivo, se debe hacer una copia de la imagen obtenida y en esta copia se realizará el análisis pertinente. Sobre la imagen original no se hará ningún tipo de procedimiento.

6.6.2. Análisis de datos digitales

[6-56] El análisis de datos digitales consiste en procesar la información recolectada a través de la aplicación de los cuatro pasos del procedimiento ya explicado anteriormente. Para tal fin, es necesario trasladar las muestras obtenidas a un laboratorio acondicionado, puesto que el procedimiento de identificación, recolección, adquisición y preservación de los datos digitales se llevó a cabo en el lugar donde se presentó el incidente de información.

[6-57] Una vez se lleve a cabo el traslado de las muestras y estas se encuentren en el laboratorio, se deben ejecutar y aplicar ciertos pasos estandarizados de manera detallada, para evitar cualquier alteración o daño de los datos.

[6-58] El análisis de los datos digitales se constituye en un procedimiento que consta de cuatro pasos que se describen a continuación:

- **Paso 1. Obtener acceso a las muestras:** si, por ejemplo, se trata de un disco duro, se lo debe extraer y aislar del sistema donde esté alojado. Si no es posible la extracción, se debe trabajar sobre el disco evitando que el sistema donde esté alojado pueda alterar el contenido de este.
- **Paso 2. Conectar la muestra a un dispositivo de lectura bloqueando la posibilidad de escritura sobre la evidencia:** lo ideal es utilizar dispositivos físicos que eviten la escritura sobre la evidencia. En el caso de utilizar sistemas basados en *software*, se evitará modificar los datos mediante la configuración adecuada (*read-only*).
- **Paso 3. Extraer de las muestras la información relevante para la averiguación:** es importante que la búsqueda de información de interés para la CI sea exhaustiva, pero, a su vez, hay que evitar presentar datos irrerelevantes. Esta búsqueda se debe hacer sobre una copia de los datos obtenidos, para evitar que se altere la muestra original. Esta copia ya ha sido hecha durante la aplicación del procedimiento anterior.
- **Paso 4. Mantener la integridad de la muestra:** en ningún momento la realización del procedimiento debe alterar la integridad de los datos digitales, ya que, si se actúa en apoyo de una investigación judicial, estos se constituyen en material probatorio, y si hacen parte de una averiguación de contrainteligencia se debe tener certeza sobre su confiabilidad y su integridad. Por tal motivo, el agente que desarrolla el análisis debe mantener en todo momento el control absoluto sobre la ubicación y los procedimientos realizados sobre las muestras. Todo esto se debe documentar de manera detallada.

**ADN BICENTENARIO****EL POLÍGRAFO, UNA HERRAMIENTA FUNDAMENTAL PARA LA CONTRAINTELIGENCIA**

Desde sus inicios, la CI del Ejército se ha valido del apoyo de dispositivos electrónicos o herramientas tecnológicas para complementar la información obtenida por medios humanos; en tal sentido, el polígrafo es una de las herramientas más efectivas para orientar la toma de decisiones.

En varias ocasiones, mediante el desarrollo de exámenes psicofisiológicos de polígrafo se ha logrado obtener información determinante para el desarrollo de operaciones de CI dirigidas a acciones de sabotaje, subversión o corrupción en el interior de la Fuerza, como lo fue el hecho presentado a finales de 2018, cuando se logró la identificación y la posterior captura de un soldado profesional que había sido infiltrado en las filas del Ejército por una organización al margen de la ley, con la intención de suministrar información clasificada de la Fuerza.

Asimismo, producto de información recolectada durante el postest de un examen de polígrafo realizado a principios de 2019, se logró determinar a los responsables de la extracción de material de guerra de una unidad militar ubicada en el noroccidente del país. En esta ocasión, los implicados eran dos soldados regulares que se encontraban prestando servicio militar, y quienes, inducidos por un suboficial del Ejército, habían hecho contacto con un grupo armado al servicio del narcotráfico que delinque en la zona del Urabá antioqueño para la entrega del armamento, el cual sería utilizado para llevar a cabo acciones terroristas en contra de la Fuerza Pública. Como resultado de la actividad poligráfica en apoyo de las operaciones de CI, se recuperó el material y se logró la identificación del personal implicado, así como su posterior captura.

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

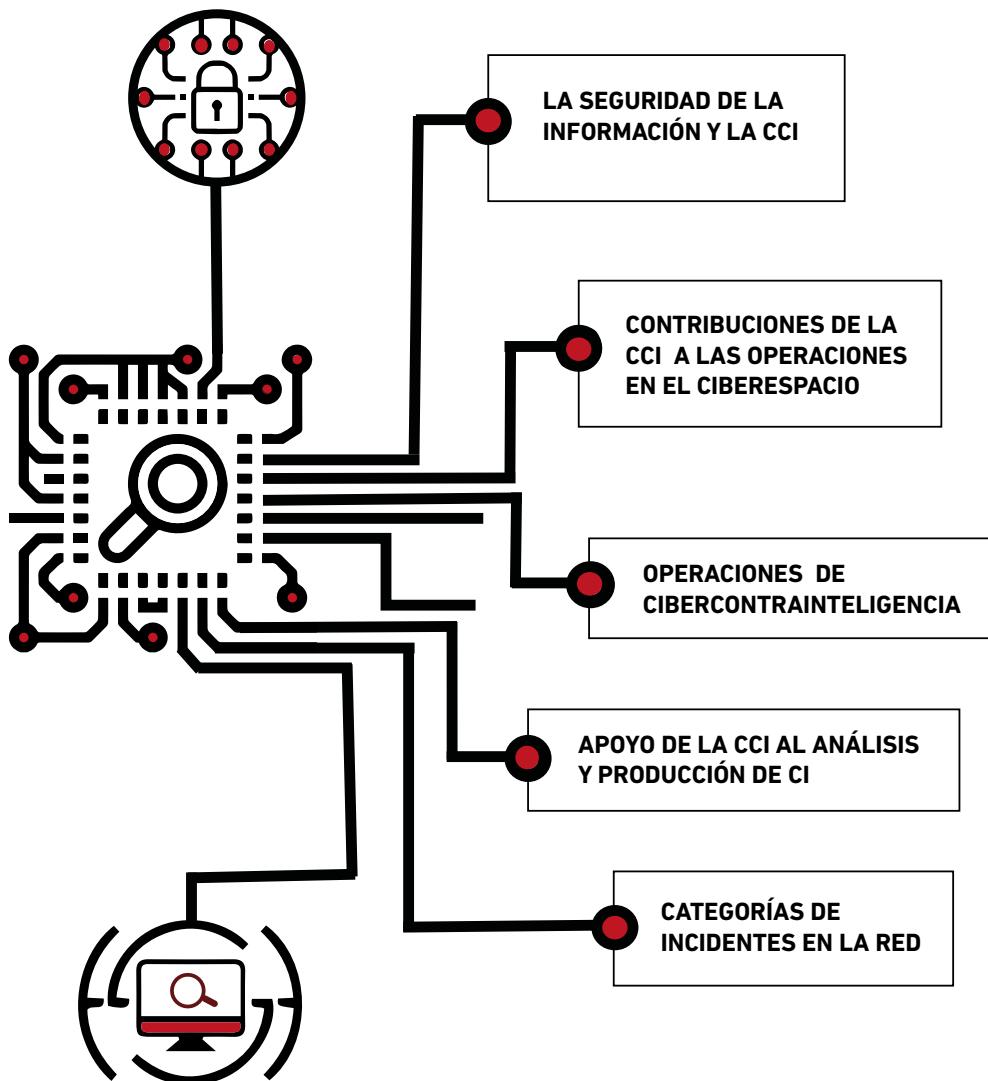
RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

CAPÍTULO 7

CIBERCONTRAINTELIGENCIA

"Solo la inteligencia se examina a sí misma".

Jaime Balmes



7.1. GENERALIDADES

[7-1] La **cibercontrainteligencia** (CCI) se define como las **actividades desarrolladas en el ciberespacio para contrarrestar las acciones de la amenaza y apoyar la recolección de información de constrainteligen**cia.

[7-2] Estas actividades se llevan a cabo mediante la ejecución de las operaciones de cibercontrainteligencia (CCI), las cuales permiten combatir fenómenos emergentes actuales o futuros tales como la subversión, el espionaje, el sabotaje y el terrorismo de tipo cibernético, incluyendo la actividad de la amenaza relacionada con el reclutamiento, la entrega de blancos o la coordinación de acciones letales y las que surjan como consecuencia de la aplicación maliciosa de los medios tecnológicos y las redes de transmisión de información y datos que afecten los intereses del Ejército.

CCI | Ciber-
constrainteligen

[7-3] Las actividades de CCI se centran en dos objetivos principales: combatir las acciones de la amenaza dirigidas a los activos críticos del Ejército que interactúen dentro del ciberespacio y apoyar la recolección de información de constrainteligencia a través de este.

7.2. PROPÓSITOS DE LA CIBERCONTRAINTELIGENCIA

[7-4] Las CCI realiza sus actividades buscando el alcance y la consolidación de los siguientes propósitos:

CI | Constrainteligen

- Recolectar información de CI en el ciberespacio.
- Contrarrestar la capacidad de la amenaza de ejecutar la recolección de información en el ciberespacio.
- Proveer cursos de acción a partir de la información recolectada como insumo para las operaciones de inteligencia, CI y las operaciones en el ciberespacio.
- Permitir el adecuado desarrollo de las operaciones en el ciberespacio.

- Recuperar o destruir información propia que se encuentre en poder de la amenaza.
- Proteger los intereses y los recursos del Ejército en el ciberespacio.

7.3. LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERCONTRAINTELIGENCIA

[7-5] Debido a la necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información propia en el ciberespacio, la CCI se hace interoperable e interdependiente de la seguridad de la información. Sin embargo, los campos de acción de estas son diferenciales, pues la seguridad de la información actúa únicamente de manera interna dentro de una red propia para prevenir, detectar y contrarrestar los riesgos y las vulnerabilidades presentes en esta, sin la necesidad de conocer las capacidades de la amenaza, y, por lo tanto, sus acciones se enmarcan dentro del concepto de "seguridad en el ciberespacio", mientras que las actividades de la CCI se enmarcan dentro del concepto de "protección del ciberespacio" y sus actividades sí requieren la identificación de amenazas específicas internas o externas, por lo cual concentran su esfuerzo en las redes o los sistemas de información del adversario (defensa activa) y su principal propósito es la recolección de información de CI en el ciberespacio que permita anticipar y contrarrestar el accionar de las amenazas en contra de los activos críticos del Ejército.

cci | Ciber-
contrainteligencia

[7-6] Tomando en cuenta que uno de los propósitos de la CCI es contrarrestar la recolección de información por parte de la amenaza, esta desarrolla una serie de técnicas y procedimientos cuya finalidad es deteriorar o destruir los elementos o las herramientas utilizados por la amenaza para llevar a cabo espionaje, sabotaje, terrorismo o subversión de tipo cibernético (ver el procedimiento de defensa activa).

[7-7] No obstante lo anterior, se requiere la aplicación de medidas defensivas que eviten el acceso no autorizado a los

sistemas de información propios, los cuales son desarrollados por la seguridad de información en apoyo a las operaciones de CCI.

7.4. CONTRIBUCIONES DE LA CIBERCONTRAINTTELIGENCIA A LAS OPERACIONES EN EL CIBERESPACIO

CCI | Ciber-
contrainteligencia

[7-8] La CCI proporciona capacidades para identificar, desinformar y contrarrestar las amenazas del dominio del ciberespacio que producen espionaje, terrorismo, sabotaje y subversión de tipo cibernético. Estos apoyos se suministrarán a través del desarrollo de técnicas propias de la disciplina de CI que se llevan a cabo como complemento del procedimiento de defensa activa.

7.4.1. Técnicas antiforenses

[7-9] Otra de las contribuciones de la CCI al desarrollo de operaciones en el ciberespacio es la aplicación de técnicas antiforenses, que son las acciones que evitan la identificación y la obtención de evidencias digitales en un proceso de investigación forense. Estas técnicas se utilizan para evitar que una amenaza que haya sido atacada obtenga información o recolecte datos que puedan determinar el origen de una explotación de vulnerabilidades realizada durante el desarrollo de una ciberoperación. De esta manera, la CCI contribuye a contrarrestar la capacidad de respuesta de la amenaza.

[7-10] La CCI se sincroniza con la seguridad de la información para configurar una estrategia que contribuya a garantizar la confidencialidad y la disponibilidad de los recursos de información que se requieren para poder ejecutar una operación en el ciberespacio.

CIBERCONTRAINTELIGENCIA

Actividades desarrolladas en el ciberespacio para contrarrestar las acciones de la amenaza y apoyar la recolección de información de contrainteligencia (MCE 2-22.1).

OPERACIONES DE CIBERCONTRAINTELIGENCIA

Acciones tácticas que permiten recolectar información de contrainteligencia, para identificar, analizar contrarrestar y neutralizar acciones de la amenaza en el ciberespacio (MCE 2-22.1).

ATAQUE CIBERNÉTICO

Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio (MCE 2-22.1).

7.5. OPERACIONES DE CIBERCONTRAINTELIGENCIA

CCI	Ciber- contrainteligencia
CI	Contrainteligencia

[7-11] Las ***operaciones de cibercontrainteligencia*** se definen como **acciones tácticas que permiten recolectar información de constrainteligenicia, para identificar, analizar contrarrestar y neutralizar acciones de la amenaza en el ciberespacio**. Estas operaciones se basan en sistemas tecnológicos y herramientas automatizadas para recolectar, explotar o neutralizar una amenaza ya sea de espionaje, de sabotaje, de subversión o de terrorismo cibernético. Dado que las amenazas en el ciberespacio son frecuentes y persistentes y tienen la capacidad de desestabilizar los sistemas del Ejército y afectar el mando tipo misión, las operaciones de CCI están diseñadas para desenvolverse en un ambiente volátil, incierto, complejo y ambiguo (VICA).

[7-12] Los agentes de CI pueden realizar estas operaciones de acuerdo con el marco jurídico y el marco doctrinal vigentes para detectar, disuadir, neutralizar o apoyar la explotación de las amenazas.

[7-13] Las operaciones de CCI incluyen actividades de recolección en el ciberespacio centradas en amenazas de ciberterrorismo, inteligencia extranjera y amenazas emergentes que puedan afectar los intereses nacionales e institucionales.

[7-14] Además de la recolección de información de CI que se lleva a cabo a través de medios humanos y técnicos, la recolección de datos en el ciberespacio se realiza principalmente a través de la web, para obtener información esencial que afecta a la operación apoyada. La recolección de CCI puede resultar de un indicio obtenido durante el desarrollo de una averiguación u operación de CI en curso, o bien, servir para iniciar nuevas averiguaciones u operaciones.

[7-15] Adicionalmente, las operaciones de CCI deben estar en capacidad de generar cursos de acción que optimicen el desarrollo de las operaciones de CI. Para ello, las operaciones de CCI desarrollan dos tareas complementarias, que contribuyen al entendimiento de la situación para su planeamiento y configuración. Estas tareas son el desarrollo del procedimiento

de defensa activa y las averiguaciones de intrusión en redes, las cuales se describen a continuación:



| **Figura 7-1 |** Procedimiento de defensa activa

7.5.1. Procedimiento de defensa activa

[7-16] La finalidad de este procedimiento es explotar y deteriorar los sistemas ciberneticos de la amenaza y recolectar información de CI en el ciberespacio. Este procedimiento siempre será desarrollado sobre servidores externos una vez haya sido identificado un factor que determine un riesgo, represente una amenaza o indique probabilidades de un ataque hacia los sistemas propios.

CI

Contrainteligencia

[7-17] El enemigo puede emplear armas sofisticadas contra objetivos específicos para atacar las debilidades nacionales

identificadas. También amenazará con emplear terrorismo, ataques indiscriminados e incluso armas químicas, biológicas, radiológicas o nucleares, dirigidas a concentraciones de unidades, centros poblados o infraestructura crítica y buscará crear efectos disruptivos orientados contra las actividades nacionales a través de ataques en el ciberespacio (MFRE 3-0). Por lo tanto, el procedimiento de defensa activa utiliza una metodología de alto nivel para interrumpir y neutralizar ataques cibernéticos. Esta provee una eficaz forma de explotar las vulnerabilidades de los atacantes, sus redes, sus nodos y sus servidores de mando y control a fin de preservar la superioridad en el ciberespacio.

[7-18] El procedimiento de defensa activa consta de cinco pasos lógicos y ordenados, donde la finalización de uno es la continuación del siguiente y una falla en el desarrollo de uno de ellos afectará significativamente el desarrollo de los demás. Por lo tanto, estos pasos y sus tareas asociadas son de obligatorio cumplimiento en aras de obtener un resultado exitoso que suministre orientación al desarrollo de las operaciones en el ciberespacio y las operaciones de CCI. El resultado de este procedimiento es el informe de análisis de defensa activa.

CCI | Ciber-
contrainteligencia

Paso 1. Planeamiento y recolección

[7-19] Este paso se refiere a la recolección de información esencial para identificar los aspectos técnicos, tanto físicos como electrónicos, que componen las redes de los adversarios y su información crítica y sensible. Esto es posible porque en la interconexión de redes existen multitud de puertos lógicos y servicios. Los más conocidos son la web y el correo electrónico, pero también hay otros, como la transmisión de ficheros, el acceso remoto, los *chats*, mensajería instantánea, la telefonía, la televisión, etc., donde, aprovechando las vulnerabilidades existentes en los enlaces técnicos y los protocolos de comunicación entre un dispositivo y otro, es posible obtener la información necesaria para identificar la composición de las redes de información y su funcionamiento.

[7-20] La recolección técnica es la actividad inicial para poder planear y ejecutar acciones en las redes y los sistemas de telecomunicaciones del adversario, y se constituye por lo mismo, en un elemento integrador de la capacidad de disuasión propia, y no solo para mantener la libertad de acción de nuestros sistemas, sino también, la voluntad de degradar la del adversario, en el momento en que se requiera. Por ello, se enfoca en obtener, analizar, valorar, centralizar, almacenar y difundir información sobre amenazas, vulnerabilidades, servicios, tendencias y capacidades de potenciales adversarios en el ambiente de la información. Se valen en primer término en el aprovechamiento de las vulnerabilidades más comunes en los sistemas de información:

- Instalaciones por defecto de sistemas y aplicaciones.
- Cuentas sin contraseñas o contraseñas poco robustas.
- La gran existencia de puertos abiertos.
- Programas de interfaz de entrada común vulnerables.
- Respaldos o *backups* incompletos o inexistentes.
- Versiones desactualizadas en sistemas operativos.

[7-21] En este paso se llevan a cabo acciones de reconocimiento que posteriormente, en la explotación, ayudan a reducir la efectividad de la amenaza menoscabando el sistema organizacional y dejando al descubierto futuras o posibles vulnerabilidades del enemigo, hasta el punto de lograr que con la degradación de los datos transmitidos el enemigo pueda cuestionar la calidad de la información de la cual dispone para tomar decisiones. Habitualmente incluye averiguaciones realizadas mediante actividades de OSINT para identificar todas las debilidades que serían potencialmente aprovechadas.

OSINT

Inteligencia de fuentes abiertas

Paso 2. Preparación y selección de objetivo

[7-22] Con toda la información obtenida en la recolección, se procede a crear las circunstancias para que el ambiente

FCG

Función de
conducción de la
guerra

ciberespacial sea configurado de acuerdo con las necesidades del comandante en relación con el desarrollo de operaciones en el ciberespacio o el apoyo a las demás FCG, según sea el caso. Esta implementación permite desarrollar la capacidad de engañar al adversario o la amenaza para ganar la iniciativa de forma anónima, y a su vez, obtener conocimiento para integrar y sincronizar los demás pasos del procedimiento, lo que da como resultado la obtención y el mantenimiento de la superioridad en el ciberespacio.

[7-23] La preparación y la selección del objetivo no son algo exclusivamente técnico, ya que requieren todo el análisis de lo obtenido en el paso anterior, con el fin de crear un perfil de la amenaza o el objetivo, puesto que es necesario ser lo suficientemente convincente y meticuloso en este intento, hasta el punto de que la amenaza no tenga otra opción que aceptar el señuelo en su sistema o red. De ahí que se recurra a varias alternativas de solución, como el uso de elementos técnicos e informáticos y la generación de sitios web o aplicaciones con fines específicos y operacionales. Esto es, en otras palabras, preparar la vía que se utilizará para realizar la intrusión al sistema de la amenaza.

[7-24] El aprovechamiento de las brechas de seguridad (vulnerabilidades en los sistemas operativos, generalmente causadas por versiones desactualizadas) identificadas en la recolección, es fundamental para poder establecer los medios y los métodos para producir los efectos deseados y obtener el acceso al sistema de información de la amenaza. Parte de estos métodos se pueden realizar de forma automatizada, y en otras ocasiones las interacciones de otras formas de introducción del señuelo serán necesarias, donde se encuentre un sistema demasiado cerrado a internet, lo que hará indispensable utilizar formas sutiles, como la ingeniería social o la preparación de medios extraíbles. La ingeniería social es el método que emplea habilidades psicológicas combinadas con herramientas tecnológicas para influenciar en una persona o en una organización, identificada en la web o en otro tipo de red, con el fin de obtener datos o información confidencial de equipos, dispositivos, procesos o personas para lograr objetivos tácticos o estratégicos.

Paso 3. Obtención de acceso

[7-25] Una vez seleccionada la vía de intrusión será posible técnicamente acceder al sistema de información de la amenaza. De esta forma se ganará la capacidad de leer y escribir datos en el sistema adversario, aunque dicho intento puede ser exitoso o no. En caso de no ser exitoso, se hará nuevamente el paso “preparación y selección del objetivo” para elegir otra vía de ingreso. Una vez logrado el acceso, mediante métodos técnicos se debe enmascarar el proceso de acceso dentro de un proceso real del sistema, migrando este a uno autorizado. Con tal método se reducirá el riesgo de ser detectado virtualmente por los sistemas de detección de intrusos del adversario o la amenaza. El estudio detallado del tipo de vulnerabilidad que se quiere aprovechar es fundamental a la hora de escoger el código a medida o el fragmento de software que se utilizará para lograr los fines del presente paso. El principal propósito de obtener acceso es atacar la confidencialidad de los sistemas de información de la amenaza.

PROCEDIMIENTO DE DEFENSA ACTIVA

- Planeamiento y recolección
- Preparación y selección de objetivo
- Obtención de acceso
- Explotación técnica y acciones sobre el objetivo
- Exfiltración

Paso 4. Explotación técnica y acciones sobre el objetivo

[7-26] La explotación se refiere a la gestión del acceso obtenido, haciendo uso de los recursos de información (IR, por su sigla en inglés) del sistema adversario comprometido, para los fines propuestos dentro de los objetivos del comandante. Esto es posible por la capacidad de implantar uno o más sistemas de mando y control en el componente de la amenaza, que se gana al obtener el acceso. Por ello, las acciones de reconocimiento del sistema mediante la exploración del sistema de archivos y la toma de evidencias, son fundamentales para desarrollar efectivamente la explotación, teniendo todo el cuidado posible para no causar daños o modificaciones a la información o los servicios del sistema del adversario, y así no generar comportamientos anómalos que alerten sobre la presencia dentro de la red.

[7-27] En la explotación se cumplen tareas de un ataque pasivo orientado a la “escucha” de las actividades del adversario o la amenaza; de ahí que en este paso se adquiera

CCI

Ciber-
contrainteligencia

la capacidad de identificar y analizar en tiempo real las acciones que pretende realizar el adversario para atacar los sistemas de información propios. Es posible obtener conocimiento de la información sobre posibles planes o acciones que se quieran ejecutar para afectar los sistemas propios en un eventual **ataque cibernético**, que se define como la **acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio**.

[7-28] También se incluyen en este grupo las tareas de postexplotación (mantener el control de la máquina para uso posterior) sobre los sistemas de la amenaza o el adversario, con el fin de ejecutar acciones sobre el sistema, de acuerdo con los requerimientos para el desarrollo de la operación de CCI y en concordancia con los objetivos que se quieran lograr. Aquí se desarrollan tareas tales como la interrupción de aplicaciones, la modificación o la creación de archivos, la alteración de información, la adición de usuarios en el sistema y la recolección de información útil. En este paso se generan conexiones inversas, que son efectivas a la hora de neutralizar las herramientas técnicas de detección de intrusiones, como los *firewalls/cortafuegos* que pueda tener desplegados el adversario.

[7-29] El propósito de la explotación es proporcionar la capacidad de atacar la disponibilidad y la integridad del sistema de información del adversario llevando a cabo tareas de degradación, alteración, interrupción, denegación y destrucción que son específicas y temporales, ejecutadas como parte de una operación ofensiva. Estas tareas collean afectar las capacidades de la amenaza, y de manera colateral, neutralizar o retrasar sus intenciones. Por lo tanto, se centran en adquirir una ventaja en el ambiente de la información, reduciendo las capacidades de respuesta de la amenaza.

[7-30] Durante este paso, es posible que se requiera ajustar algunos objetivos en virtud del tipo de acceso que se haya logrado, pues no siempre se ingresa con privilegios de administrador, y de ahí se desprende que una de las principales tareas por desarrollar sea el *escalado de privilegios*, que consiste en adquirir la mayor cantidad de atributos para el

manejo de archivos y usuarios con el fin de instalar o modificar configuraciones de manera discreta.

Paso 5. Exfiltración

[7-31] Este paso es importante, en la medida en que significa abandonar el sistema de información de la amenaza y la terminación de las tareas asociadas al procedimiento de defensa activa, sin dejar rastro alguno o huella digital que permita a la amenaza establecer las acciones realizadas por los sistemas ciberneticos del Ejército. Para ello, se realizan tareas de borrado de huellas en el sistema, así como la terminación de los procesos y los servicios que se utilizaron, dejando abierta la posibilidad de acceder nuevamente al sistema en caso de no haberse desarrollado una degradación o destrucción de activos de información. La norma general en el desarrollo del procedimiento de defensa activa es su temporalidad, ya que se desarrollará por una sola vez sobre el sistema objetivo, y luego de cumplido el propósito del comandante, se desliga cualquier enlace remoto con los sistemas de ataque propios (ver el anexo E).

7.5.2. Averiguaciones de intrusión en redes

[7-32] Las averiguaciones de intrusión en las redes del Ejército implican la recolección, el procesamiento y el análisis de datos digitales relacionadas con las penetraciones del adversario en los sistemas de información del Ejército. Estas averiguaciones de CI, generalmente, se llevan a cabo independientemente de las demás actividades de recolección de información de CI. Sin embargo, dados los asuntos jurídicos que involucran a internet, las averiguaciones de intrusión en la red pueden requerir cooperación con otras entidades gubernamentales y de inteligencia de gobiernos extranjeros.

CI

Contrainteligencia

[7-33] Las amenazas a los sistemas de información del Ejército pueden aprovechar las vulnerabilidades existentes para penetrar en los sistemas computarizados del Ejército y

recolectar información reservada o clasificada mediante personal confiable, que, voluntaria o inconscientemente, permita que las fuerzas adversarias exploten estos recursos críticos de infraestructura. Cualquier amenaza con el motivo, los medios, la oportunidad y la intención de hacer daño representa un riesgo potencial. Las amenazas a los recursos de información del Ejército pueden incluir la interrupción, la degradación, la denegación, la extracción, la destrucción, la corrupción, la explotación o el acceso no autorizado a redes y sistemas de información. Los agentes de CI están especialmente capacitados para detectar y contrarrestar estas amenazas.

[7-34] Una averiguación de intrusión de la red puede iniciarse en las siguientes circunstancias, pero no necesariamente, limitarse a ellas:

- Intrusiones detectadas o intentos de intrusión en sistemas de información clasificados o no clasificados por personas no autorizadas.
- Materialización de incidentes que comprometan la confidencialidad de la información de inteligencia y de CI.
- Materialización de incidentes que comprometan la integridad o la disponibilidad de los recursos informáticos conectados a la red.
- Asignación de privilegios a usuarios no autorizados.

CI | Contrainteligencia

[7-35] Los propósitos de llevar a cabo una averiguación de intrusión en la red serán:

- Identificar completamente las entidades o los actores involucrados.
- Determinar el alcance y el impacto de la intrusión.
- Identificar el objetivo de la amenaza.
- Determinar las herramientas, las técnicas y los procedimientos utilizados por la amenaza.

- Ayudar a las autoridades judiciales, conforme al artículo 43 de la Ley 1621 de 2013, a determinar el alcance de los daños a los intereses de la nación y el Ejército.

[7-36] Si la intrusión en la red se origina en el interior de la Fuerza y existen indicios de subversión, el comando superior puede tomar acciones disciplinarias o administrativas, según el caso, o solicitar la intervención de autoridades judiciales para llevar a cabo un proceso en contra del implicado y permitir la neutralización o la explotación de la amenaza. Si se determina que la actividad no constituye una amenaza para la seguridad nacional, y es de carácter puramente penal, la unidad afectada remitirá el asunto a las autoridades judiciales competentes y la CI brindará los apoyos que sean de su especialidad.

7.6. ACTIVIDADES INTERAGENCIALES DE CIBERCONTRAINTELIGENCIA

[7-37] La CCI deberá disponer de los medios humanos, físicos o digitales que garanticen un enlace para el intercambio de información con las agencias militares, civiles gubernamentales y no gubernamentales, dentro de la AU y la UNESI, con el fin de optimizar las actividades de recolección de información de interés cibernético y coordinar, confirmar, desvirtuar o complementar las operaciones de CI. Estas actividades de enlace se llevan a cabo para garantizar que la configuración del ambiente operacional en el ciberespacio sea complementada con información de otras agencias que también desarrollan capacidades en el ciberespacio.

[7-38] Los agentes de CI podrán llevar a cabo entrevistas, siempre y cuando la misión lo requiera, para obtener información relacionada con las capacidades de recolección de inteligencia de la amenaza o de sus actividades de identificación y selección de objetivos que puedan afectar los intereses nacionales o de la nación anfitriona en el ciberespacio. Los agentes de CI que hacen este tipo de entrevistas pueden apoyar el planeamiento de operaciones, las actividades de protección de la

CI | Contrainteligencia

CCI	Ciber-contrainteligencia
AU	Acción unificada
UNESI	Unión de esfuerzos de inteligencia

información, la seguridad de las operaciones y las actividades de engaño militar.

[7-39] Los agentes trabajan en conjunto con otras agencias o dependencias durante las operaciones de CCI para apoyarse en las fuentes humanas que puedan suministrar información relacionada con las capacidades de la amenaza en el ciberespacio.

7.7. APOYO DE LA CIBERCONTRAINTELIGENCIA AL ANÁLISIS Y LA PRODUCCIÓN DE CONTRAINTELIGENCIA

[7-40] El análisis de CI se utiliza para proporcionar evaluaciones exhaustivas oportunas, precisas y pertinentes sobre la inteligencia de la amenaza, que afecte los intereses del Ejército, con el fin de proteger al personal, las instalaciones, la infraestructura, los equipos, el material y la información.

CCI | Ciber-
contrainteligencia

[7-41] El análisis de CCI es una actividad exclusivamente técnica. El dominio cibernetico difiere del dominio terrestre en que se compone de redes y servidores interconectados a nivel mundial, lo que lo hace mucho más complejo y volátil. Además del análisis de CI sobre las organizaciones, las operaciones terroristas y otras amenazas, se requiere un conocimiento técnico detallado de los sistemas de información, de las redes del Ejército y de la red mundial de información (web).

PSPB | Proceso de
selección y
priorización de
blancos

[7-42] Las operaciones de CCI consisten en el desarrollo de actividades de inteligencia, vigilancia, reconocimiento, apoyo al PSPB y desarrollo de apreciaciones de CI del ciberespacio. Por tal motivo, los análisis de CCI deben proporcionarse de forma oportuna a los comandantes apoyados durante el planeamiento de una operación, suministrando información de interés para el PMTD relacionada con la capacidad de la amenaza para emplear recursos a través del ciberespacio. El análisis de CCI se lleva a cabo en todos los niveles de la guerra.

7.8. CATEGORÍAS DE INCIDENTES EN LA RED

[7-43] Los incidentes en las redes informáticas del Ejército son eventos voluntarios o involuntarios que ocurren dentro del segmento de la red integrada de comunicaciones (RIC) que administra el Ejército, y pueden alterar la disponibilidad de los recursos informáticos que la componen.

[7-44] Se identifican por categoría, según el tipo de incidente que se produzca. Si se tipifica como un delito, se deberá aplicar la ley penal vigente, sin perjuicio de las competencias disciplinarias. Si se determina que el incidente es de naturaleza interna o corresponde con el *modus operandi* de la amenaza, la CI procederá a realizar la averiguación o la operación pertinente, de acuerdo con las categorías de incidentes relacionados con la red informática, que se muestran en la tabla 7-1.

[7-45] Como mínimo, las incidencias de las categorías 1, 2, 4 y 7 se informan a la CI. Todos los incidentes que impliquen un compromiso potencial o real de sistemas o redes clasificadas se informan a través de los canales de comunicación autorizados.

[7-46] El reporte de incidentes ciberneticos debe contener la siguiente información relevante, cuando esté disponible:

- Intruso y víctimas en el sistema.
- Dirección IP de origen y ruta al sistema víctima utilizado por el intruso.
- Propietario de la dirección IP de origen.
- Fecha y hora de la intrusión y duración del acceso del intruso al sistema.
- Grado de acceso obtenido por el intruso (privilegios de administrador o *root*).
- Nivel de clasificación, función (por ejemplo, servidor web, servidor de nombres de dominio), sistema operativo y dirección IP del sistema de víctimas.

CI

Contrainteligencia

IP

Protocolo de internet

- Cualquier sistema de seguridad externo.
- Técnica utilizada en el incidente o la intrusión.
- Explicación detallada de cómo la técnica utilizada logró la explotación del sistema atacado.
- Si la técnica explotó una vulnerabilidad conocida en el sistema de información; proporcionar detalles sobre la vulnerabilidad.
- Si el sistema tenía disponible un parche de seguridad o actualización que podría haber evitado el incidente y por qué no se utilizó el parche.
- Si la técnica se utiliza para orientar otros sistemas o redes en relación con otras víctimas.
- Historia de la técnica, donde se especifique si esta ha sido utilizada en ataques anteriores por *hackers* conocidos u otras organizaciones.
- Resultados de la averiguación sobre el incidente, si la hubo.
- Alcance del daño, tanto real como potencial, causado por el incidente.
- Cualquier vínculo entre el incidente y cualquier incidente anterior en los sistemas del Ejército.
- Si el sistema atacado ha sido víctima de incidentes anteriores (proporcionar detalles).

| Tabla 7-1 | Categorías de incidentes relacionados con la red informática

CATEGORÍA	DESCRIPCIÓN
CATEGORÍA 1	Intrusión de nivel raíz (incidente). Acceso privilegiado no autorizado (de administrador o <i>root</i>) a un sistema del Ejército.
	Intrusión de nivel de usuario (incidente). Acceso no privilegiado no autorizado (permisos de nivel de usuarios) a un sistema del Ejército. Las herramientas automatizadas, las explotaciones dirigidas o la lógica malintencionada de propagación automática también pueden obtener estos privilegios.
CATEGORÍA 2	Intento fallido de actividad (evento). Intentar obtener acceso no autorizado al sistema, que es derrotado por mecanismos defensivos normales. El intento no consigue acceder al sistema (por ejemplo, el atacante intenta combinaciones de nombre de usuario y contraseña válidas o potencialmente válidas) y la actividad no se puede caracterizar como exploratoria. Puede incluir informes de código malicioso en cuarentena.
	Denegación de servicio (incidente). Actividad que dificulta, impide o detiene la funcionalidad normal de un sistema o red.
CATEGORÍA 3	Actividad de incumplimiento (evento). Esta categoría se utiliza para actividades que, debido a las acciones del Ejército (configuración o uso), hacen que los sistemas sean potencialmente vulnerables (por ejemplo, parches de seguridad de misión, conexiones a través de dominios de seguridad, instalación de aplicaciones vulnerables). En todos los casos, esta categoría no se utiliza si se ha producido un compromiso real. La información que se ajusta a esta categoría es el resultado de cambios de configuración no conforme, incorrecta o manejo imprudente por parte de usuarios autorizados.
	Reconocimiento (evento). Una actividad (exploración o sondeo) que busca identificar una computadora, un puerto abierto, un servicio abierto o cualquier combinación para su posterior explotación. Esta actividad no resulta directamente en un compromiso.
CATEGORÍA 4	Lógica malintencionada (incidente). Instalación de software malicioso (por ejemplo, troyano, puerta trasera, virus o gusano).
	Investigación (evento). Los eventos potencialmente maliciosos o anómalos que se consideren sospechosos y que justifiquen o estén en proceso de revisión. Ningún evento se cerrará como categoría 8. La categoría 8 se volverá a clasificar en las categorías apropiadas 1 a 7 o 9 antes del cierre.
CATEGORÍA 5	Explicación de la anomalía (suceso). Los eventos que inicialmente se sospecha son maliciosos, pero después de la investigación se determina que no se ajustan a los criterios para ninguna de las otras categorías (por ejemplo, mal funcionamiento del sistema).
CATEGORÍA 6	
CATEGORÍA 7	
CATEGORÍA 8	
CATEGORÍA 9	

7.9. INDICADORES DE INTERÉS CIBERNÉTICO

[7-47] Las vulnerabilidades existentes en las redes informáticas del Ejército y los incidentes que ocurren a diario como consecuencia de la explotación voluntaria o involuntaria de las mismas, alteran la interconexión entre los recursos de la red y generan registros que deben ser identificados y evaluados. A continuación, se enumeran algunos indicadores que pueden ser de interés para la CCI:

- Datos cifrados.

- Tiempos o fallos inusuales de inicio de sesión.
- Modificación no autorizada de archivos de sistema y registros.
- Modificación no autorizada de las reglas de *firewall*.
- Conectividad inexplicable: física o de red.
- *Hardware* y *software* anómalos.
- Tarjeta de interfaz de red configuradas en modo promiscuo o *sniffer*.
- Tráfico de red inusual en la red interna.
- Actividad de escaneo, interna o externa.
- Vulnerabilidades no corregidas después de varias notificaciones.
- Interés inusual en la configuración de redes o sistemas (topologías, *firewalls*, medidas de seguridad, relaciones de confianza).
- Interés inusual en la penetración o pruebas de vulnerabilidad.
- Cuentas ocultas inexplicables o con niveles de privilegio.
- Intentos de introducir *software* malicioso.
- Intentos de obtener una excepción a la directiva de seguridad.
- Intentos no autorizados de obtener accesos.
- Intentos de escalar privilegios dentro de la red.
- Intentos iniciados por el fabricante para instalar o actualizar *hardware* o *software*.
- Actividad o conectividad inexplicable de programas o procesos.

- Almacenamiento inexplicable de archivos cifrados.
- Conexiones de módem no autorizadas.
- Conectividad externa excesiva, inusual o inexplicable (red o módem).

7.10. MANEJO DE DISPOSITIVOS COMPROMETIDOS EN UN INCIDENTE CIBERNÉTICO

[7-48] La averiguación de cualquier actividad que pueda ser de interés para una operación de CI puede producir evidencia electrónica o digital. Los dispositivos comprometidos pueden ir desde un computador de escritorio hasta un dispositivo móvil: por ejemplo, celulares, *tablet*, USB, CD, consolas o sistemas de videojuegos conectados a la televisión con *chip* de grabación incorporado.

CI

Contrainteligencia

[7-49] Las imágenes, los archivos de audio o de texto y otros datos de estos medios se pueden alterar o destruir fácilmente. Es imperativo que los agentes de CI busquen, identifiquen, protejan y aseguren tales dispositivos de acuerdo con los parámetros legales establecidos para el manejo de evidencia, y sin pasar por alto las restricciones establecidas por la ley. Las siguientes preguntas se consideran una guía para obtener más información de un incidente:

- ¿Está relacionado el incidente con capturas de tráfico de red?
- ¿La amenaza logró obtener el *software* o el *hardware* del sistema atacado?
- ¿Es el sistema informático una herramienta de la amenaza?
- ¿El sistema fue activamente utilizado por el implicado para cometer el incidente?
- ¿Se usaron identificadores falsos u otros documentos falsificados con el equipo, el escáner o la impresora?

- ¿El sistema informático se utiliza para almacenar evidencia de la amenaza?
- ¿Se obtuvieron datos digitales que relacionen el dispositivo implicado en el incidente con organizaciones terroristas o grupos al margen de la ley?
- ¿El intruso usó el dispositivo electrónico para atacar otros sistemas o para almacenar información robada del Ejército?

[7-50] Una vez identificado el propósito del equipo de cómputo o del dispositivo electrónico en el incidente, es necesario responder las siguientes preguntas:

- ¿Hay causa suficiente para solicitar el apoyo de autoridades judiciales que desarrollen el proceso de cadena de custodia?
- ¿Hay una causa probable para captar datos?

[7-51] Donde se realizará la búsqueda:

- ¿Es práctico realizar procedimientos en el mismo lugar donde se presentó el incidente, o debe hacerse el examen en un laboratorio?
- ¿Es esencial para el proceso de recolección de información hacer copias de *bite a bite* de los discos duros comprometidos?
- Teniendo en cuenta los datos de almacenamiento masivo en los sistemas de hoy, ¿cómo los expertos en computación forense buscarán los datos de manera eficiente y oportuna?

7.11. OTROS ASPECTOS PARA TENER EN CUENTA EN LA RECOLECCIÓN DE INFORMACIÓN

[7-52] En el desarrollo de una averiguación u operación de CCI probablemente se identificarán dispositivos electrónicos de diferente tipo que pueden contener datos necesarios para orientar la toma de decisiones o información relevante asociada a un incidente de interés para la CI. Estos pueden ser:

- GPS
- Accesorios o elementos domésticos conectados a una red (internet de las cosas).
- Consolas de videojuegos.
- Cámaras digitales.
- Grabadoras digitales.
- Quemadores de CD.
- Fotocopiadoras.
- Fax.
- Contestadoras automáticas.
- Teléfonos inalámbricos.

CI

Contrainteligencia

[7-53] Tenga en cuenta las siguientes medidas de precaución si va a manipular los dispositivos anteriormente relacionados:

- Si el dispositivo está encendido, no lo apague: apagar el dispositivo podría activar una función de bloqueo. El cargador de alimentación, los cables de alimentación y cualquier periférico que pertenezca al dispositivo pueden ayudar a que este permanezca encendido.
- Si el dispositivo está apagado, no lo encienda: encenderlo podría alterar la evidencia en el dispositivo.
- Documente toda la información en pantalla y fotografíe si es posible.

- Aproveche el manual de instrucciones de cada uno de los dispositivos.
- Estos sistemas pueden estar conectados a la red, pueden ser independientes o pueden ser portátiles.
- Algunos sistemas en red contienen discos duros internos que almacenan imágenes.
- Pueden contener datos incluyendo texto, imágenes y mapas.
- Pueden contener información de acceso a internet.
- Generalmente, contienen rutas y lugares marcados.
- Pueden contener una capacidad de radio bidireccional.
- Pueden tener capacidad telefónica.
- Pueden hacer un seguimiento de las líneas de tiempo.
- Se pueden encontrar como parte integrante de otros dispositivos portátiles (por ejemplo, teléfonos celulares, miniportátiles, PC portátiles y cámaras digitales).



Todo dispositivo que cuente con una memoria interna puede almacenar archivos para los que no está diseñado. Ejemplo: una grabadora de audio digital puede almacenar archivos de texto o imagen multimedia.

[7-54] Los dispositivos electrónicos que contienen los vehículos también pueden suministrar información relevante en el desarrollo de una operación de CCI, pues al igual que cualquier otro dispositivo electrónico tradicional, pueden contener datos almacenados como texto, imágenes, mapas, audio, información de acceso a internet, capacidades telefónicas, rutas, ubicaciones marcadas, líneas de tiempo y correos electrónicos.

[7-55] Los medios de almacenamiento se utilizan para contener datos de un dispositivo electrónico. Algunos dispositivos tienen un espacio de almacenamiento fijo ubicado dentro sí mismos. Esta forma de almacenamiento requiere un medio de interconexión con otra fuente para transferir los datos cuando sea necesario. Muchos dispositivos de hoy en día tienen capacidades tanto para el almacenamiento fijo (interno) como para la memoria y la capacidad de almacenar datos solo o simultáneamente en medios de almacenamiento extraíbles. Los medios extraíbles se utilizan para transferir y almacenar datos.

[7-56] Los dispositivos de almacenamiento de datos electrónicos vienen en muchas variedades, y existe una gran cantidad de dispositivos modernos que no son utilizados con frecuencia. Aunque hay algunos estándares, la siguiente lista incluye algunos de los tipos de medios más comunes y bien establecidos que se encuentran en el mercado de consumo y son comerciales:

- Disco flexible.
- Minidisco.
- Discos duros de estado sólido.
- Disco duro externo.
- Disco compacto (CD) LS-120 (súper disco).
- *Microdrive*.
- USB.
- Micro USB.
- *Pendrive*.
- Tarjeta de memoria.



ADN BICENTENARIO

SABOTAJE CIBERNÉTICO

En 2017, una brigada del Ejército Nacional ubicada en el sur del país emite un requerimiento a la CI del Ejército informando acerca de algunas fallas de seguridad identificadas en la red de datos, lo que, según expresaban los encargados de seguridad informática de la unidad, había generado incidentes de fuga de información. En consecuencia, el Comando de Contrainteligencia designa una unidad especializada para llevar a cabo procedimientos de cibercontrainteligencia (CCI) en las instalaciones de la brigada, gracias a lo cual se pudo identificar una vulnerabilidad crítica en el rango de direcciones IP asignadas a uno de los batallones subordinados que se hallaba en zona fronteriza. Por tal motivo, el equipo de CI destinado a la misión se despliega en el área de interés, donde logran identificar que la unidad contaba con un servicio de internet comercial de un proveedor colombiano, el cual se valía de la infraestructura tecnológica del país vecino para proveer los servicios que solicitaba la unidad.

Este hallazgo conllevó identificar una acción de sabotaje (con fines desconocidos) por parte de un funcionario de la unidad, quien hizo una conexión clandestina entre el servicio de internet comercial y la red del Ejército, la cual era desconectada manualmente cada vez que se generaba un reporte del departamento de comunicaciones CEDE6. Aunque se logró mitigar el impacto, este evento llegó a vulnerar por completo la seguridad de la información digital de la división a la que pertenecían las unidades comprometidas, pues se generó un enlace que permitía que la información de carácter reservado del Ejército fluyera por la infraestructura tecnológica suministrada por otro país, lo cual pudo haber interferido el tráfico de red y poner en riesgo la seguridad nacional.

ANEXO A

**NIVEL DE CLASIFICACIÓN
INFORME DE CONTRAINTELIGENCIA
ANEXO A**

RESTRICCIÓN DE DIFUSIÓN DE LA INFORMACIÓN

Informe recolección de información	Interno	<input type="checkbox"/> Externo <input type="checkbox"/>
N.º de Registro		
Lugar	Fecha	
Unidad		
Receptor		
I. Marco operacional		
II. Enemigo		
III. Información recolectada		
IV. Análisis		
V. Pertinencia		
VI. Recomendaciones		
VII. Anexos		
<p><i>Nota aclaratoria:</i> para el informe externo, no aplica los ítems <u>marco operacional y anexos</u></p> <hr/> <p style="text-align: center;">Código de operación del recolector de información o analista</p> <p><i>Elaboró:</i></p> <p><i>Revisó:</i></p> <p><i>Vo.Bo:</i></p>		

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACION NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

**R E S T R I N G I D O
P A R A U S O E X C L U S I V O D E L C E D O E**

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

ANEXO B

NIVEL DE CLASIFICACIÓN
INFORME DE RECOLECCIÓN DE INFORMACIÓN
ANEXO B

RESTRICCIÓN DE DIFUSIÓN DE LA INFORMACIÓN

Informe recolección de información:		Inicial	<input type="checkbox"/>	Avance	<input type="checkbox"/>
N.º de registro					
Lugar				Fecha	
Unidad					
Receptor					
I. Marco operacional					
II. <input type="checkbox"/> Procedencia de la información				<input type="checkbox"/> Tiempo empleado	
III. Información recolectada					
IV. Recursos administrativos					
V. Recomendaciones					
<p>Nota aclaratoria: para el informe inicial, no aplica el ítem <u>tiempo empleado</u> para el informe de avance, no aplica el ítem <u>procedencia de la información</u></p> <hr/> <p style="text-align: center;">Código de operación del recolector de información o analista</p>					
<p><i>Elaboró:</i></p> <p><i>Revisó:</i></p> <p><i>Vo. Bo:</i></p>					

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedará por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACIÓN NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

ANEXO C

**NIVEL DE CLASIFICACIÓN
INFORME DE RESULTADOS
ANEXO C**

RESTRICCIÓN DE DIFUSIÓN DE LA INFORMACIÓN

Informe recolección de información:		I nterno <input type="checkbox"/>	E xterno <input type="checkbox"/>
Nº Registro			
Lugar		Fecha	
Unidad			
Receptor			
I. Ubicación			
II. Tipo de operación			
III. Resultados			
Comandante de la unidad táctica			
<i>Elaboró:</i> Comandante de Compañía. <i>Revisó:</i> Oficial de operaciones. <i>Vo.Bo:</i>			

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. LA PRESENTE INFORMACIÓN NO CONSTITUYE PRUEBA NI ANTECEDENTES (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

ANEXO D

**NIVEL DE CLASIFICACIÓN
INFORME DE CIERRE
ANEXO D**

RESTRICCIÓN DE DIFUSIÓN DE LA INFORMACIÓN

Informe de cierre			
N.º de Registro			
Lugar		Fecha	
Unidad			
Receptor			
I. Marco operacional			
II. Enemigo			
III. Información recolectada			
IV. Acciones tomadas			
V. Concepto jurídico			
VI. Conclusiones			
Comandante de la unidad táctica			
<i>Elaboró:</i> Comandante de compañía <i>Revisó:</i> Oficial de operaciones <i>Vo. Bo:</i> Asesor jurídico			

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACIÓN NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE

ANEXO E**NIVEL DE CLASIFICACIÓN****INFORME ANÁLISIS DEFENSA ACTIVA
ANEXO E****RESTRICCIÓN DE DIFUSIÓN DE LA INFORMACIÓN**

Lugar donde se realizan las actividades:	Fecha: (AA-MM-DD)	
Unidad a la que se le realiza el análisis:		
Comandante, jefe y/o director: (Grado, nombres y apellidos)		
Personal que realizó el acompañamiento: (Grado, nombres y apellidos)		
Motivo para el desarrollo del trabajo:	N.º de oficio o solicitud	Fecha: (AA-MM-DD)

N.º	Generalidades sobre la unidad o instalación
1.	Introducción:
1.1	
1.2	Ubicación:
1.3	Antecedentes:

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACION NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

NIVEL DE CLASIFICACIÓN
INFORME ANÁLISIS DEFENSA ACTIVA
ANEXO E

N.º	Planificación y recolección
2.	Descripción
2.1	
N.º	Preparación y selección del objetivo
3.	Descripción
3.1	
N.º	Obtener acceso
4.	Resultado
4.1	
N.º	Explotación técnica y acciones sobre el objetivo
5.	Resultado
5.1	

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACIÓN NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

NIVEL DE CLASIFICACIÓN
INFORME ANÁLISIS DEFENSA ACTIVA
ANEXO E

N.º	Exfiltración
6.	Descripción
6.1	
7. Observaciones	
1. 2. 3. 4. 5.	
8. Recomendaciones	
1. 2. 3. 4.	

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACION NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

CONTRAINTELIGENCIA
MCE 2-22.1

NIVEL DE CLASIFICACIÓN
INFORME ANÁLISIS DEFENSA ACTIVA
ANEXO E

Firma y postfirma del responsable de la misión
(Grado, nombres y apellidos)

Distribución

Original: Unidad solicitante

Copia: Unidad generadora del Informe

COMPROMISO DE RESERVA. La información contenida en el presente documento goza de Reserva Legal, razón por la cual todo servidor público que tenga acceso a su contenido, quedara por el mismo hecho cobijado de las obligaciones impuestas en la Ley Estatutaria 1621 de 2013 Capítulo VI, su divulgación o usos no autorizados conllevará las sanciones de tipo penal disciplinarias y/o fiscal pre establecidas en los Códigos vigentes para la revelación ilícita de confidencial. **LA PRESENTE INFORMACIÓN NO CONSTITUYE PRUEBA NI ANTECEDENTES** (Art. 248 C.N). Es el producto del análisis de múltiples documentos e intercambios de informaciones a través de los convenios celebrados con diferentes Entidades Estatales.

NIVEL DE CLASIFICACIÓN

GLOSARIO

1. ABREVIATURAS, SIGLAS Y ACRÓNIMOS

ABREVIATURA, SIGLA Y/O ACRÓNIMO	SIGNIFICADO	ACRÓNIMO EN INGLÉS (OTAN*)	SIGNIFICADO
AD	Acción decisiva	---	<i>Decisive action</i>
ADAC	Apoyo de la defensa a la autoridad civil	DSCA	<i>Defense support of civil authorities</i>
AO	Área de operaciones	*A00	<i>Area of operations</i>
AU	Acción unificada	---	<i>Unified Action</i>
CACIM	Comando de apoyo de combate de contrainteligencia militar	---	---
CE	Contraespionaje	CE	<i>Counterespionage</i>
CI	Contrainteligencia	CI	<i>Counterintelligence</i>
CT	Contraterrorismo	CT	<i>Counterterrorism</i>
CCI	Cibercontrainteligencia	CCA	<i>Cyber Counterintelligence activity</i>
CI2CM	Centro Integrado de Información de Contrainteligencia Militar	---	---
COA	Curso de acción (por su sigla en inglés)	*COA	<i>Course of action</i>

* AAP-15(2013) "NATO GLOSSARY OF ABBREVIATIONS USED IN NATO DOCUMENTS AND PUBLICATIONS". En aras de la interoperabilidad, muchas siglas se mantienen en el idioma inglés.

ABREVIATURA, SIGLA Y/O ACRÓNIMO	SIGNIFICADO	ACRÓNIMO EN INGLÉS (OTAN*)	SIGNIFICADO
COIN	Contrainsurfencia	COIN	<i>Counterinsurgency</i>
DDHH	Derechos Humanos	---	<i>Human rights</i>
DIH	Derecho Internacional Humanitario	*IHL	<i>International Humanitarian Law</i>
EEIPT	Elementos esenciales de información de las propias tropas	EEFI	<i>Essential elements of friendly information</i>
EEM	Espectro electromagnético	EMS	<i>Electromagnetic spectrum</i>
EW	Guerra electrónica (por su sigla en inglés)	EW	<i>Electronic Warfare</i>
FCG	Función de conducción de la guerra	---	<i>Warfighting function</i>
FF. MM.	Fuerzas Militares	---	<i>Military forces</i>
FID	Defensa interna en el extranjero (por su sigla en inglés)	FID	<i>Foreign Internal Defense</i>
FISS	Inteligencia extranjera y servicios de seguridad (por su sigla en inglés)	FISS	<i>Foreign intelligence and security services</i>
GEOINT	Inteligencia geoespacial (por su sigla en inglés)	---	<i>Geospatial Intelligence</i>
HUMINT	Inteligencia humana (por su sigla en inglés)	HUMINT	<i>Human Intelligence</i>
IR	Recursos de información (por su sigla en inglés)	IR	<i>Information Resources</i>
ISR	Inteligencia, vigilancia y reconocimiento (por su sigla en inglés)	ISR	<i>Intelligence, surveillance, and reconnaissance</i>
JIC	Junta de inteligencia conjunta	---	---
LRC	Lista de recursos críticos	CAL	<i>Critical asset list</i>

ABREVIATURA, SIGLA Y/O ACRÓNIMO	SIGNIFICADO	ACRÓNIMO EN INGLÉS (OTAN*)	SIGNIFICADO
LRD	Lista de recursos defendidos	DAL	<i>Defended assets list</i>
MASINT	Inteligencia de medidas y huellas distintivas (por su sigla en inglés)	* MASINT	<i>Measurement and signature intelligence</i>
MEDES	Medida de eficacia	*MOE	<i>Measure of effectiveness</i>
MEDEF	Medida de desempeño	MOP	<i>Measure of performance</i>
MRI	Medios de recolección de información	---	---
MTM	Mando tipo misión	---	<i>Mission Command.</i>
ORDOP	Orden de operaciones	*OPORD	<i>Operation Order</i>
OPSEC	Seguridad de las operaciones	OPSEC	<i>Operations Security</i>
OSINT	Inteligencia de fuentes abiertas (por su sigla en inglés)	OSINT	<i>Open Source Intelligence</i>
OT	Organizaciones terroristas	ITO	<i>International terrorist organizations</i>
OTAN	Organización del Tratado del Atlántico Norte	NATO	<i>North Atlantic Treaty organization</i>
OTU	Operaciones terrestres unificadas	---	<i>Unified land operations</i>
PDD	Examen psicofisiológico de polígrafo (por su sigla en inglés)	PDD	<i>Psychophysiological detection of deception</i>
PICC	Preparación de inteligencia en el campo de combate	IPB	<i>Intelligence preparation of the Battlefield</i>
PMTD	Proceso militar de toma de decisiones	MDMP	<i>Military decision-making process</i>
PRODOP	Proceso de operaciones	---	<i>Operations process</i>
PSPB	Proceso de selección y priorización de blancos	---	<i>Targeting</i>

ABREVIATURA, SIGLA Y/O ACRÓNIMO	SIGNIFICADO	ACRÓNIMO EN INGLÉS (OTAN*)	SIGNIFICADO
RDA	Revista después de la acción	*AAR	<i>After action review</i>
RIC	Red integrada de comunicaciones	---	---
RICC	Requerimientos de información crítica de comandante	CCIR	<i>Commander's critical information requirement</i>
ROM	Rango de las operaciones militares	ROMO	<i>Range of military operations</i>
SI	Solicitud de información	RFI	<i>Request for information</i>
SIGNIT	Inteligencia de señales (por su sigla en inglés)	SIGNIT	<i>Signals Intelligence</i>
SOP	Procedimientos operacionales estandarizados (por su sigla en inglés)	*SOP	<i>Standard operating procedure</i>
TECHINT	Inteligencia técnica (por su sigla en inglés)	TECHINT	<i>Technical Intelligence</i>
TOE	Tablas de organización y equipo	*TOE	<i>Tables of organization and equipment</i>
UNESI	Unión de esfuerzos de inteligencia	---	---
VOCADOC	Vocabulario doctrinal	---	---

2. TÉRMINOS¹

Acción decisiva (AD): combinación continua y simultánea de tareas ofensivas, defensivas, de estabilidad o de apoyo de la defensa a la autoridad civil (MFRE 3-0).

***Activos críticos del Ejército:** conjunto de recursos que representan o generan un valor, compuesto por instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnología de la información, cuya inhabilitación o destrucción tendría un impacto negativo para el Ejército.

***Agente:** en el ámbito de la inteligencia, es un oficial, suboficial, soldado o civil (dado de alta por el Ministerio de Defensa Nacional como auxiliar de inteligencia), quien se encuentra autorizado, capacitado y entrenado para desarrollar actividades de inteligencia o contrainteligencia.

***Agente local:** persona que posee acceso a información reservada o clasificada y puede entregar información de forma voluntaria o involuntaria.

Amenaza: cualquier combinación de actores, entidades o fuerzas que tienen la capacidad y la intención de afectar las fuerzas amigas, los intereses nacionales o la nación (MFRE 3-0).

***Anticorrupción:** conjunto de actividades diseñadas para combatir la omisión, extralimitación o acción irregular de las funciones de miembros de la Fuerza que busquen recibir algún beneficio que no corresponda a la ética y la moral.

Antiterrorismo (AT): medidas defensivas utilizadas para reducir la vulnerabilidad de las personas y los bienes en caso de actos terroristas; su objetivo es suprimir el terrorismo mediante una acción rápida por parte de las fuerzas militares y de las autoridades civiles y locales (MCE 3-24.0).

Apoyo de la defensa a la autoridad civil (ADAC): soporte proporcionado por las Fuerzas Militares de Colombia y todas las instituciones que integran el sector defensa, en respuesta a solicitudes de asistencia de las autoridades civiles nacionales para emergencias domésticas de cualquier índole, apoyo a la imposición de la ley y otras actividades con entidades calificadas para situaciones especiales (MFE 3-28).

***Ataque cibernético:** acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio.

¹ Los términos que esta publicación propone están señalados con un asterisco y los tomados de otros manuales están acompañados de su correspondiente referencia en paréntesis.

***Averiguaciones:** actividad de constrainteligencia enfocada a confirmar o desvirtuar los indicadores de los incidentes de seguridad.

***Características biométricas:** rasgos biológicos y de comportamiento distintivos de una persona que se pueden utilizar para el reconocimiento automatizado.

***Ciberconstrainteligencia:** actividades desarrolladas en el ciberspace para contrarrestar las acciones de la amenaza y apoyar la recolección de información de constrainteligencia.

Competencia distintiva: capacidad esencial y perdurable que un arma o una organización proporciona a las operaciones del Ejército (MFE 1-01).

Cooperación en seguridad: toda interacción entre el Ministerio de Defensa Nacional y los organismos de defensa extranjeros, que tiene como objetivo crear relaciones que promueven intereses específicos en materia de defensa y seguridad, con el fin de desarrollar capacidades militares aliadas para las operaciones de defensa mutua y multinacional (MFRE 3-0).

***Contraespionaje:** acción que tiene como finalidad negar al adversario el acceso a la información reservada o clasificada del Ejército o de los asociados de la acción unificada.

Contrainsurficia (COIN): esfuerzos civiles y militares realizados para derrotar una insurgenza y hacer frente a posibles daños importantes (MFRE 3-05).

Constrainteligencia (CI): conjunto de actividades destinadas a la preservación de personal, instalaciones, infraestructura, equipos, material e información que están encaminadas a identificar, prevenir, detectar, interrumpir, explotar, contrarrestar, disuadir, desinformar y neutralizar la recolección de información de inteligencia extranjera y servicios de seguridad, organizaciones terroristas, agentes locales y otras amenazas (MFRE 2-0).

***Constrainteligencia institucional:** función de constrainteligencia que busca identificar y contrarrestar las acciones de corrupción al interior de la fuerza.

***Constrainteligencia multilateral:** función de constrainteligencia que dirige y desarrolla sus actividades para apoyar la seguridad nacional, defensa nacional y seguridad pública.

***Contrasabotaje:** acción de contrarrestar el daño, deterioro o destrucción total o parcial del poder de combate, los activos críticos del Ejército o la infraestructura crítica de la nación.

***Contrasubversión:** acción de contrarrestar el desarrollo de actividades del enemigo, que busquen debilitar la competencia, el carácter, el compromiso, la cultura, la ética y la moral del Ejército o de los asociados de la acción unificada.

Contraterrorismo: acciones militares ofensivas para prevenir, detener y responder a las acciones terroristas, atacando en forma directa su infraestructura y redes de apoyo y de manera indirecta para influenciar ambientes regionales y globales para restringir su empleo por parte de redes terroristas (MFRE 3-05).

***Debriefing:** actividad que busca obtener información a través de preguntas sistemáticas con respecto a un tema en particular.

Decepción: conjunto de medidas dirigidas a inducir al error al enemigo por medio de la manipulación, la deformación o la falsificación de evidencias para hacerle actuar de forma perjudicial a sus intereses (MFRE 3-37).

Defensa interna en el extranjero (FID): participación de las agencias civiles y militares de un gobierno, en cualquiera de los programas de acción adoptados por otro gobierno u otra organización designada para liberar y proteger su sociedad de la subversión, la anarquía, la insurgencia, el terrorismo y de otras amenazas a su seguridad (MFRE 3-0).

Defensa nacional: protección de la soberanía, el territorio, la población nacional y la infraestructura de defensa crítica de Colombia contra las amenazas externas y la agresión u otras amenazas según las indicaciones del presidente (MFRE 3-0)

Elementos esenciales de información de las propias tropas (EEIPT): aspectos críticos de la operación de las propias tropas que de ser conocidos por el enemigo comprometerían, llevarían al fracaso o limitarían el éxito de la operación; por lo tanto, deben ser protegidos de la detección por parte de este (MFRE 2-0).

Explotar: tarea ofensiva que usualmente sigue a la conducción de un ataque exitoso y está diseñada para desorganizar al enemigo en profundidad (MFRE 3-90).

Función de conducción de la guerra (FCG): conjunto de tareas y sistemas (personas, organizaciones, información y procesos) unidos por un propósito común que los comandantes utilizan para cumplir misiones y objetivos de entrenamiento (MFE 3-0).

Guerra electrónica (EW): acción militar que implica el uso de energía electromagnética y dirigida para controlar el espectro electromagnético o para atacar al enemigo (MFRE 3-0).

***Indicios de constrainteligencia:** información inicial que de acuerdo con el análisis de constrainteligencia podría representar una posible acción de la inteligencia de la amenaza.

***Infiltración:** En inteligencia, técnica que emplea la amenaza para introducir una persona dentro de una organización con el fin de obtener información.

***Informática forense:** aplicación de técnicas especializadas para obtener, preservar o restablecer datos que han sido procesados digitalmente y almacenados en un dispositivo electrónico.

Informe de inteligencia y constrainteligencia: documento en el cual se plasma el resultado del análisis de informaciones de inteligencia o constrainteligencia. Se emplea para actualizar y presentar un panorama específico al comandante para la toma de decisiones (MFRE 2-0)

Insurgencia: acciones de un grupo o movimiento organizado, normalmente ideológicamente motivado, que busca afectar o prevenir un cambio político o derrocar una autoridad gubernamental dentro de un país o región, enfocado en persuadir o coaccionar a la población mediante el uso de la violencia y la subversión (MCE 3-24.0).

Inteligencia de fuentes abiertas (OSINT): disciplina complementaria de la inteligencia producida a partir de información públicamente disponible que es recolectada, explotada y difundida oportunamente a una audiencia apropiada con el propósito de atender un requerimiento específico de inteligencia (MFRE 2-0).

Inteligencia de medidas y huellas distintivas (MASINT): inteligencia obtenida mediante el análisis cuantitativo y cualitativo de datos (métricos, angulares, espaciales, de longitud de onda, de modulación, de plasma e hidromagnéticos) derivados de sensores técnicos específicos, a fin de identificar el rasgo distintivo de una fuente emisora o receptora de ondas electromagnéticas y facilitar el reconocimiento y/o la medición de la misma (MFRE 2-0).

Inteligencia de múltiples fuentes: integración de inteligencia e información relevante para analizar situaciones o condiciones que impactan en las operaciones (MFRE 2-0).

Inteligencia de señales (SIGINT): inteligencia derivada de señales de instrumentación de comunicaciones, electrónicas y extranjeras (MFRE 2-0).

Inteligencia geoespacial (GEOINT): explotación y el análisis de imágenes e información geoespacial para describir, evaluar y visualizar las características físicas y las actividades geográficamente referenciadas en la tierra (MFRE 2-0).

Inteligencia humana (HUMINT): recolección de información mediante el empleo de medios humanos entrenados, capacitados y certificados para la obtención de información sobre amenazas (identifica sus elementos, intenciones, composición, fortaleza, disposiciones, tácticas, equipos y capacidades), terreno, clima y consideraciones civiles (MFRE 2-0).

Inteligencia técnica (TECHINT): inteligencia derivada de la recolección, el procesamiento, el análisis y la explotación de datos e información referentes a equipos y materiales externos, con el fin de prevenir sorpresas tecnológicas, evaluar capacidades científicas y técnicas extranjeras y desarrollar contramedidas para neutralizar las ventajas tecnológicas de un adversario (MFRE 2-0).

Inteligencia, vigilancia y reconocimiento (ISR): actividades que se sincronizan e integran al planeamiento y la utilización de sensores, medios de recolección de información y el procesamiento, explotación y difusión en apoyo directo a las operaciones actuales y futuras (MFE 2-0).

Inteligencia: producto de someter la información al proceso de inteligencia (MFRE 2-0).

***Inteligencia extranjera:** organización de carácter secreto que recolecta información reservada o clasificada.

***Misión de trabajo:** documento legal que regula las actividades de inteligencia y contra-inteligencia, emitido por los directores de los organismos o jefes de unidad, sección o dependencia.

Neutralizar: tarea táctica de la misión que tiene como resultado la incapacidad del personal o material del enemigo para interferir en una operación particular (MCE 3-90.1).

Nivel estratégico: **1.** Nivel de la guerra en el cual una nación, a veces como miembro de un grupo de naciones, determina los objetivos y la orientación de seguridad estratégica nacional o multinacional (en una alianza o coalición), luego desarrolla y utiliza los recursos nacionales para alcanzar esos objetivos (MFC 1.0). **2.** Establece los objetivos nacionales, multinacionales y del teatro (MFE 1-01).

Nivel operacional: **1.** Nivel de la guerra en el que se planean, conducen y sostienen campañas y operaciones mayores para cumplir los objetivos estratégicos dentro de teatros u otras áreas operacionales (MFC 1.0). **2.** Unifica el empleo táctico de las fuerzas con los objetivos estratégicos nacionales y militares a través del diseño de campañas y operaciones mayores (MFE 1-01).

Nivel táctico: nivel en el que se planean y ejecutan las batallas y los combates para alcanzar los objetivos militares asignados a las unidades tácticas o fuerzas de tarea (MFE 1-01).

Niveles de la guerra: marco para definir y clarificar la relación entre los objetivos nacionales, el enfoque operacional y las tareas tácticas (MFE 1-01).

Operación: 1. Acción militar o ejecución de una misión militar estratégica, operacional, táctica, de fuerza, entrenamiento o administrativa (MFE 1-01). 2. Secuencia de acciones tácticas con un propósito común o un tema unificador (MFE 1-01).

***Operaciones de cibercontrainteligencia:** acciones tácticas que permiten recolectar información de contrainteligencia, para identificar, analizar, contrarrestar y neutralizar acciones de la amenaza en el ciberespacio.

***Operaciones de contrainteligencia:** secuencia de acciones tácticas para la recolección de información sobre las acciones de inteligencia de la amenaza y los indicios de corrupción al interior de la fuerza.

Orden de operaciones: directriz emitida por un comandante a sus comandantes subordinados con el propósito de coordinar efectivamente la ejecución de una operación (MFE 1-01).

***Penetración:** en inteligencia, técnica que emplea la amenaza para lograr que una persona ejecute acciones adversas a la organización a la que pertenece.

Preparación de inteligencia del campo de combate (PICC): proceso sistemático de análisis de las variables de la misión de enemigo, terreno, clima y consideraciones civiles en un área de interés para determinar su efecto en las operaciones (MFRE 2-0).

Proceso de selección y priorización de blancos (PSPB): conjunto de actividades interrelacionadas para seleccionar y analizar la acción o el ataque adecuado contra un blanco, teniendo en cuenta las necesidades y capacidades operacionales (MFE 3-09).

Proceso militar para la toma de decisiones (PMTD): metodología de planeamiento cílico para entender la situación y la misión, desarrollar cursos de acción, seleccionar el más oportuno y producir un plan u orden de operaciones (MFE 5-0).

Requerimiento de información crítica del comandante (RICC): requerimiento de información identificado por el comandante como crítico para facilitar una toma de decisiones oportuna (MFRE 2-0).

Requerimiento de información de las propias tropas (RIPT): información que el comandante y el estado mayor/plana mayor necesitan para entender el estado de las propias tropas y de las capacidades de apoyo (MFRE 5-0).

Sabotaje: daño o deterioro que se hace en instalaciones, productos, etc., o procedimiento de lucha contra la autoridad (contra los patronos, el Estado o las fuerzas de ocupación en conflictos sociales o políticos) (MCE 3-24.0).

Seguridad de las operaciones (OPSEC): proceso de identificación, análisis y protección de la información crítica durante el proceso de operaciones (MFRE 3-37).

Seguridad militar: capacidad militar basada en el análisis y diagnóstico de amenazas, riesgos y vulnerabilidades relacionados con la seguridad de personas, seguridad física, seguridad de información y seguridad de la infraestructura crítica, dirigida a recomendar medidas activas y/o pasivas contra posibles acciones de una amenaza (MFRE 3-37).

Seguridad nacional: esfuerzo nacional concertado para prevenir los ataques terroristas, reducir las vulnerabilidades a estos, atender desastres naturales y otras emergencias (MFRE 3-0).

Seguridad pública: actividades de prevención, detección y neutralización frente a amenazas de crimen organizado y delitos nacionales, transnacionales e internacionales, que atenten contra las condiciones de bienestar de la población civil, la prosperidad de las comunidades, la infraestructura y servicios asociados al Estado incluyendo los recursos naturales (MFRE 3-0).

***Servicios de seguridad:** organizaciones público-privadas que desarrollan actividades asociadas con la seguridad y/o la recolección de información.

Subversión: conjunto de acciones diseñadas para debilitar la fortaleza o la moral militar, económica, psicológica o política de una autoridad gobernante (MCE 3-24.0).

***Sonsacamiento:** técnica discreta de entrevista, que no le permite al entrevistado conocer la intención específica del agente.

***Suplantación:** técnica utilizada para sustituir de manera ilegal un elemento, sistema o persona para obtener algún beneficio.

Táctica: empleo y disposición ordenada de unidades en relación con otras (MFE 1-01).

Tarea: acción o actividad claramente definida y específicamente asignada a un individuo u organización que se debe ejecutar por estar impuesta por una autoridad competente (MFE 1-01).

Tarea defensiva: tarea conducida para derrotar un ataque enemigo, ganar tiempo, economizar fuerzas y desarrollar condiciones favorables para tareas ofensivas o de estabilidad (MFRE 3-0).

Tarea ofensiva: tarea conducida para derrotar y destruir fuerzas enemigas, capturar terreno, recursos y centros poblados (MFRE 3-0).

Tarea de estabilidad: aquella que se conduce dentro o fuera del territorio nacional, en coordinación con otros instrumentos del poder nacional, para mantener o restablecer un ambiente seguro y proporcionar servicios esenciales de gobierno, reconstrucción de infraestructura de emergencia y asistencia humanitaria (MFRE 3-0).

Terrorismo: uso ilegal de la violencia o de la amenaza de violencia, a menudo motivado por creencias religiosas, políticas o ideológicas, para difundir terror e imponer a los gobiernos o las sociedades la búsqueda de objetivos generalmente políticos (MCE 3-24.0).

***Vigilancia electrónica:** uso de dispositivos electrónicos para controlar o monitorear actividades, comunicaciones, sonidos o impulsos electrónicos.

REFERENCIAS

Colombia, Congreso de la República (2013). Ley Estatutaria 1621, "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones". Recuperada de <http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf>

Colombia. Presidencia de la Republica (2015). Decreto 1070, "por el cual se expide el Decreto Único Reglamentario del Sector Administrativo de Defensa". Recuperada de <http://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=62256>

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 1-01, *Doctrina*, Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 3-0, *Operaciones*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 3-05, *Operaciones Especiales*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 3-07, *Estabilidad*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 2-0, *Inteligencia*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 3-28, *Apoyo de la defensa a la autoridad civil*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental del Ejercito 3-37, *Protección*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental de Referencia del Ejercito 1-02, *Términos y Símbolos*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental de Referencia del Ejercito 2-0, *Inteligencia*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental de Referencia del Ejercito 3-0, *Operaciones*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental de Referencia del Ejercito 3-05, *Operaciones Especiales*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2017). Manual Fundamental de Referencia del Ejercito 3-37, *Protección*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2018). Manual de Campaña del Ejercito 3-24.0, *Guerra Irregular*. Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2009). *Manual de Seguridad Militar EJC 2-4-1* (2.a ed.). Bogotá: Ejército Nacional.

Colombia, Ejército Nacional (2005). Manual EJC 2-18 *Cómo evitar la infiltración y penetración del enemigo*. Bogotá: Ejército Nacional.

NATO (2010). AAP-15 *Glossary of abbreviations used in NATO documents and publications*.

ONU (1999). Resolución 1269, del Consejo de Seguridad de la Organización de las Naciones Unidas. Recuperada de http://www.cienciaspenales.net/files/2016/10/4_42E49838CB-8503C0E04015AC20201354.pdf

US ARMY (2009). FM 2-22.2 *Counterintelligence*.

PÁGINA DEJADA EN BLANCO INTENCIONALMENTE

MCE 2-22.1

CONTRAINTELIGENCIA



CEDOC

COMANDO DE
EDUCACIÓN Y DOCTRINA



CEDOE

CENTRO DE DOCTRINA
DEL EJÉRCITO

RESTRINGIDO
PARA USO EXCLUSIVO DEL CEDOE