LA CIBERDEFENSA EN COLOMBIA

Mayor MILENA ELIZABETH REALPE DIAZ
Jefe de Prospectiva y Cooperación del Comando Conjunto Cibernético - CCOC

Bogotá, 29 de Noviembre de 2017

LINEAMIENTOS NACIONALES

2011

Documento

Conpes 3701

Consejo Nacional de Política Económica y Social
República de Colombia
Departamento Nacional de Planeación

2014

476 Plan Nacional de Desarrollo 2014-2018:
Todos por un nuevo país

Fortalecimiento de las capacidades en ciberdefensa: Colombia debe desarrollar capacidades que permitan atender las amenazas cibernéticas y sus riesgos asociados, así como fortalecer las capacidades de neutralización y reacción ante incidentes o ataques cibernéticos que afecten contra la infraestructura crítica digital y la soberanía nacional. Para ello, se desarrollarán las siguientes líneas de acción:

- Caracterización del esquema de identificación y categorización de la infraestructura crítica digital y establecer los planes de protección de esa infraestructura.
- Fortalecimiento de las capacidades ofensivas del país en el ciberespacio y posicionamiento de Colombia en la región como referente en ciberdefensa.

2016

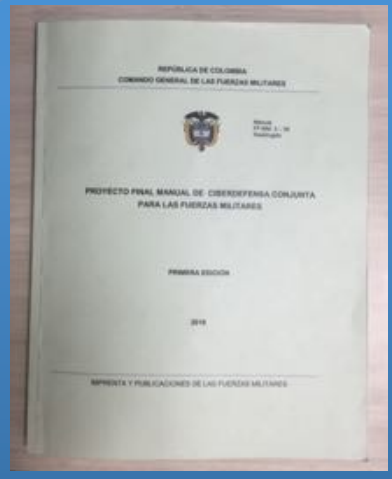
Documento

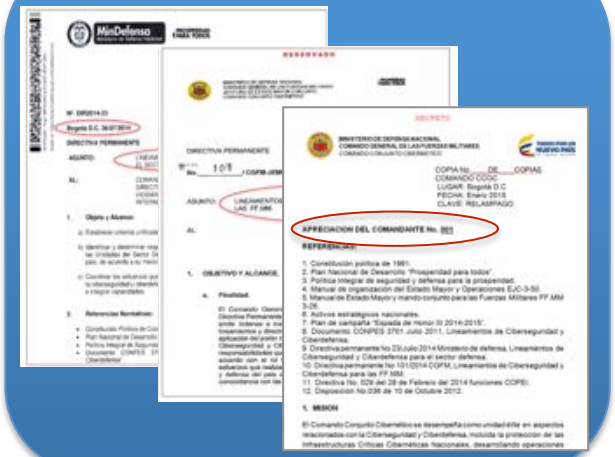
CONPES 3854

Consejo Nacional de Política Económica y Social
República de Colombia
Departamento Nacional de Planeación

FUNDAMENTO LEGAL

Artículo 217 de la CPC

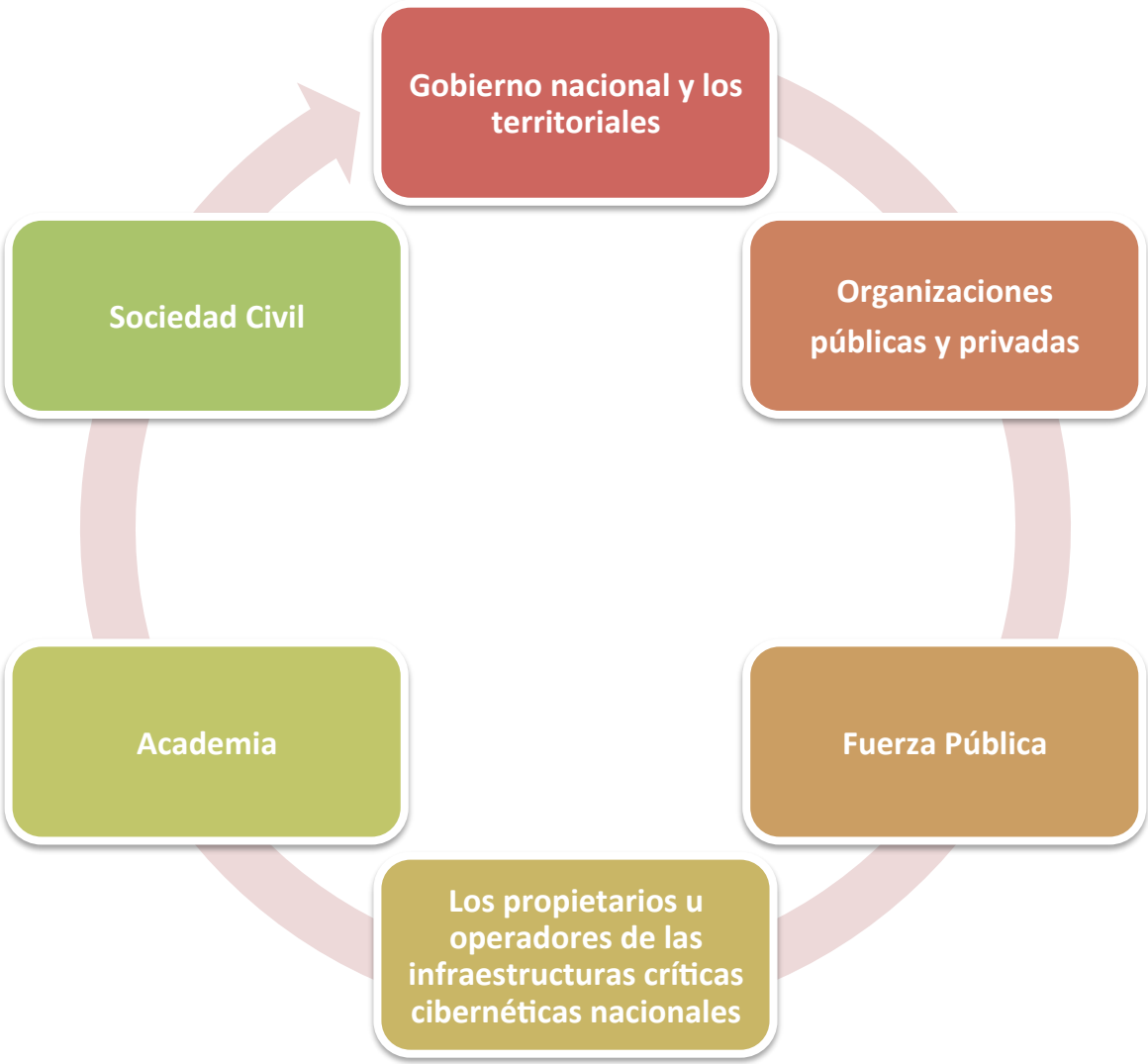




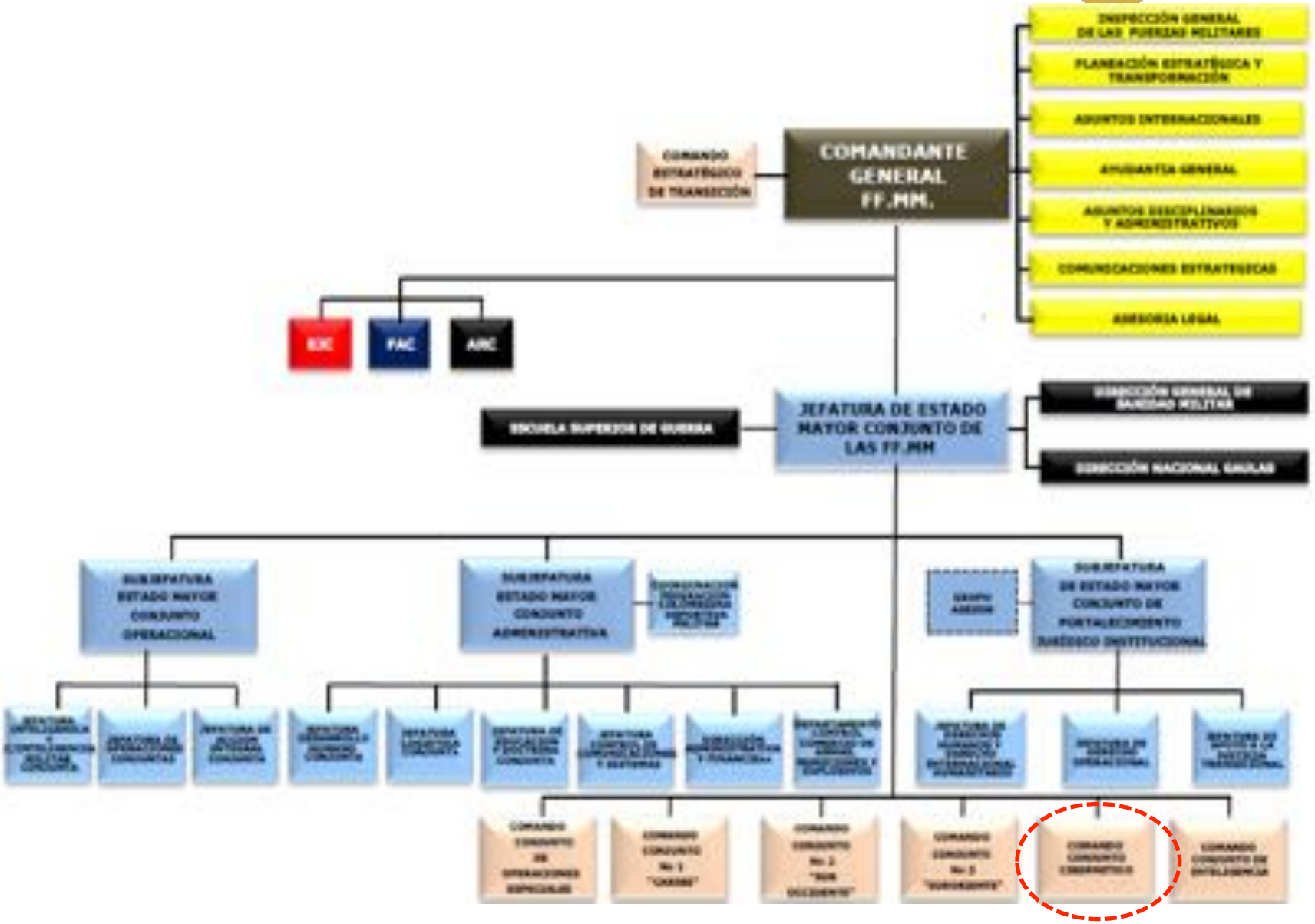
INSTITUCIONALIDAD CONPES 3701

INSTITUCIONALIDAD CONPES 3854

MULTIPLES PARTES INTERESADAS



ORGANIZACIÓN MDN



FUNCIONES Y RESPONSABILIDADES

Implementar una Estrategia de Ciberdefensa para el país, basado en personas, tecnologías y procesos.

(**Operaciones Militares** en el Ciberespacio).

Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.

Ciberdefensa de la infraestructura crítica del País en el ámbito Cibernético, incluida la del Sector Defensa.

UNIDADES MILITARES CIBERNÉTICAS

Unidad Cibernética Ejército Nacional

Unidad Cibernética Armada Nacional

Unidad Cibernética Fuerza Aérea

- Integración de capacidades de Ciberdefensa
- Operaciones Conjuntas en el Ciberespacio.
- Investigación, innovación y desarrollo en Ciberseguridad y Ciberdefensa.
- Ciberdefensa de la Infraestructura Critica Cibernética.

CONTEXTO INTERNACIONAL

No.	PAÍS	SIGLA	NOMBRE
1	EE.UU	USCYBERCOM	UNITED STATES CYBER COMMAND
		FCC-C10F	US FLEET CYBER COMMAND
		ARCYBER	ARMY CYBER COMMAND
		AFCYBER	AIR FORCES CYBER/24TH AIR FORCE
2	COLOMBIA	CCOC	COMANDO CONJUNTO CIBERNÉTICO
		UCEJC	UNIDAD CIBERNÉTICA EJÉRCITO
		UCARC	UNIDAD CIBERNÉTICA ARMADA
		UCFAC	UNIDAD CIBERNÉTICA FUERZA AÉREA
3	ARGENTINA	EMCFFAA	COMANDO CONJUNTO CIBERDEFENSA
4	VENEZUELA	DICOCIBER	DIRECCIÓN CONJUNTA DE CIBERDEFENSA
5	ECUADOR	COCIBER	COMANDO DE CIBERDEFENSA (En Proceso de Activación)
6	PERÚ	CODEC	COMANDO OPERACIONAL DEL CIBERESPACIO (En Proceso de Activación)
7	URUGUAY	CERT-Militar	CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA MILITAR. (En Proceso de Activación)
8	BRAZIL	CDCIBER	CENTRO DE DEFENSA CIBERNETICA (EJÉRCITO)
9	MÉXICO	CCCC	CENTRO DE CONTROL DE CIBERDEFENSA Y CIBERSEGURIDAD (ARMADA - En Proceso de Activación)
10	CHILE	CIC	COMITÉ INTER MINISTERIAL DE CIBERSEGURIDAD
11	CANADA	CCIRC	CENTRO DE RESPUESTAS A INCIDENTES CIBERNETICOS
12	BOLIVIA	N/A	NO CUENTA CON CIBERCOMANDOS
13	PARAGUAY	N/A	NO CUENTA CON CIBERCOMANDOS

COMANDOS CONJUNTOS

UNIDADES DE LAS FUERZAS

ORGANIZACIONES CIVILES

ALINEACIÓN NACIONAL Y SECTORIAL

DNP

Fortalecimiento de las capacidades de Ciberdefensa

MDN

Objetivo 4: Combatir las nuevas y tempranas expresiones del crimen organizado que amenacen la seguridad y el funcionamiento transparente del Estado.

Objetivo 5: Garantizar la soberanía e integridad del territorio nacional, protegiendo los intereses nacionales

CGFM

Objetivo 2: Alcanzar y mantener la superioridad en todas las operaciones a través de la integración de las capacidades militares.

Objetivo Específico 2.3: Adquirir la superioridad militar en el ciberespacio a través de la integración de capacidades de ciberseguridad y Ciberdefensa de las FF.MM.

PLAN ESTRATÉGICO MILITAR DE ESTABILIZACIÓN Y CONSOLIDACIÓN "VICTORIA" - CONCEPTO GENERAL

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

ESTADO FINAL 07-AGO-18

Pilares

Líneas Estratégicas

Moral y Bienestar	Educación y Doctrina	Logística y Eficiencia Administrativa	DIH y DIDH	Capacidades Estratégicas

1. Control Institucional del Territorio

1. APOYAR el proceso del DDR.
2. DINAMIZAR el control militar.
3. INCREMENTAR esfuerzos conjuntos, coordinados, interinstitucionales y combinados.

2. Fortalecimiento Institucional

4. CONSOLIDAR la legitimidad y la seguridad jurídica integral.
5. INTENSIFICAR mecanismos de prevención y control.

3. Cooperación y Desarrollo

6. ARTICULAR las capacidades de las Fuerzas Militares con los esfuerzos interinstitucionales.
7. POTENCIAR las capacidades propias.

Objetivos estratégicos

- Proporcionar las condiciones de seguridad necesarias para apoyar el proceso del DDR.
- Potenciar el control terrestre, marítimo, fluvial, aéreo y ciberespacio; y hacer irreversibles los logros alcanzados.
- Contribuir a la disuasión y derrota de las amenazas persistentes y emergentes.
- Fortalecer y mantener la integridad institucional.
- Fortalecer la transparencia.
- Contribuir al desarrollo Nacional.
- Participar en misiones humanitarias, internacionales y de protección ambiental.

Alcanzar condiciones favorables de seguridad; y contribuir a la estabilización y consolidación de una paz estable y duradera.

Fuerzas Militares modernas, fortalecidas y motivadas para enfrentar amenazas internas y externas en escenarios simultáneos, contribuyendo al desarrollo del país y al mantenimiento de la seguridad regional e internacional.

PLAN DE DEFENSA NACIONAL

LÍNEAS ESTRATÉGICAS Y OBJETIVOS INTERMEDIOS

EJE 1. Control Institucional del Territorio

	Objetivos estratégicos
1. APOYAR el proceso del DDR.	**Proporcionar las condiciones de seguridad necesarias para apoyar el proceso del DDR.**
1. **Entrenar y capacitar** tropas para desempeñarse en el proceso de seguridad del DDR.	
2. **Disuadir y neutralizar** amenazas armadas en las Zonas Veredales Transitorias de Normalización ZVTN y Puntos Transitorios de Normalización PTN.	
3. **Contribuir** en la seguridad de los desplazamientos relacionados con el DDR.	
2. DINAMIZAR el control militar.	**Potenciar el control terrestre, marítimo, fluvial, aéreo y del ciberespacio; y hacer irreversibles los logros alcanzados.**
4. **Intensificar** el control territorial en antiguas áreas de influencia de las FARC	
5. **Incrementar** el control militar e institucional del territorio nacional.	
6. **Proteger** la infraestructura crítica y activos estratégicos de la nación.	
7. **Fortalecer** el control en las fronteras terrestres, fluviales, marítimas y el espacio aéreo.	
8. **Proteger** el ciberespacio.	
3. INCREMENTAR esfuerzos conjuntos, coordinados, interinstitucionales y combinados.	**Contribuir a la disuasión y derrota de las amenazas persistentes y emergentes.**
9. **Focalizar e incrementar** el esfuerzo principal contra el ELN.	
10. **Enfrentar** los GAO/SAP de manera sistémica.	
11. **Neutralizar** las fuentes de financiación de los GAO y la amenaza persistente.	
12. **Contribuir** a la desaparición de las economías ilícitas.	
13. **Apoyar** el combate a los fenómenos de criminalidad.	
14. **Contribuir** en la contención de las migraciones irregulares.	

LÍNEAS ESTRATÉGICAS Y OBJETIVOS INTERMEDIOS

Objetivos estratégicos

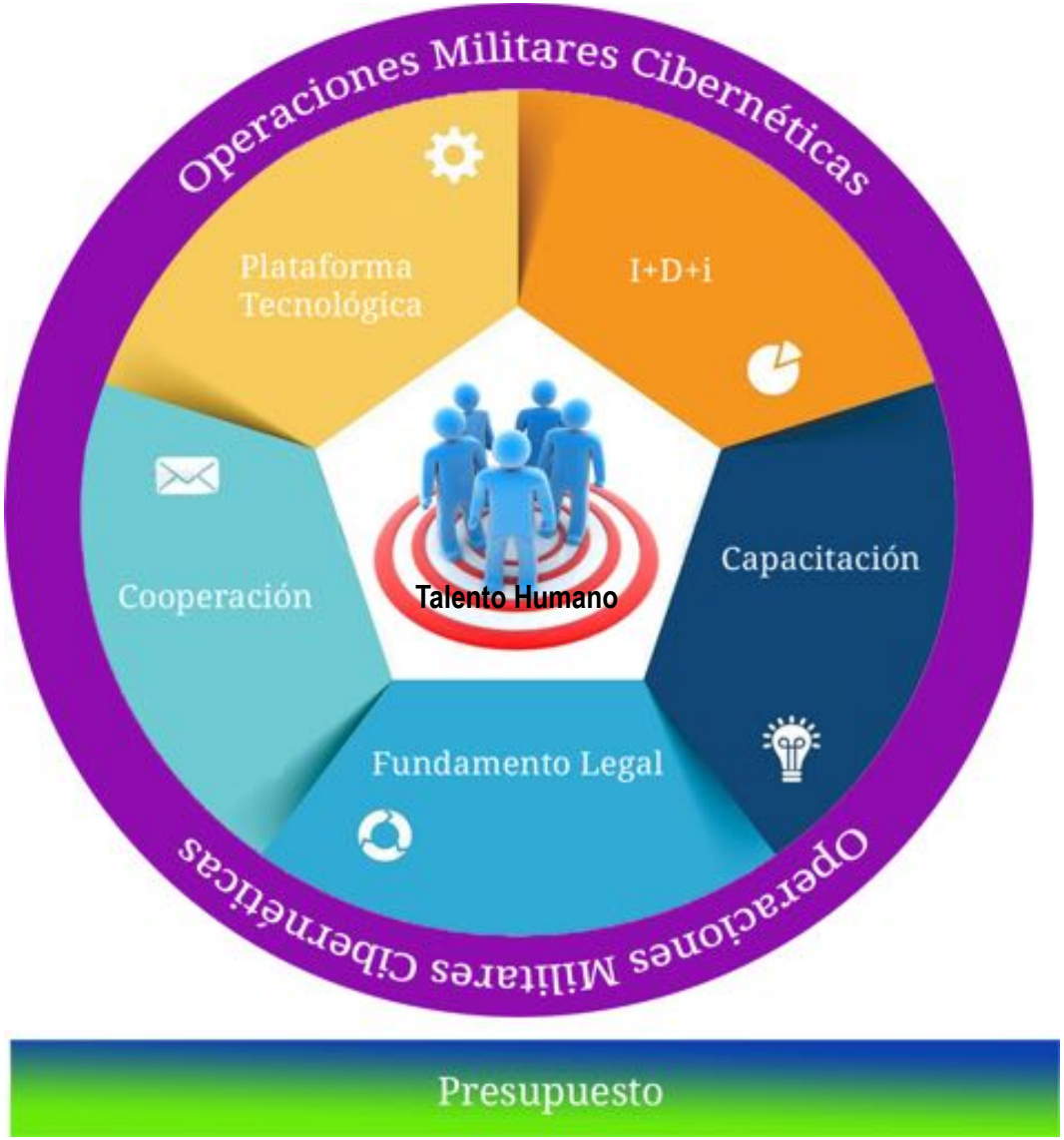
EJE 1. Control Institucional del Territorio

2. DINAMIZAR el control militar.

Potenciar el control terrestre, marítimo, fluvial, aéreo y del ciberespacio; y hacer irreversibles los logros alcanzados.

4. **Intensificar** el control territorial en antiguas áreas de influencia de las FARC
5. **Incrementar** el control militar e institucional del territorio nacional.
6. **Proteger** la infraestructura crítica y activos estratégicos de la nación.
7. **Fortalecer** el control en las fronteras terrestres, fluviales, marítimas y el espacio aéreo.
8. **Proteger** el ciberespacio.

EJES FUNDAMENTALES



CENTRO DE OPERACIONES CIBERNÉTICAS

SOC:

Prevenir, identificar, tratar, neutralizar y responder ante ataques cibernéticos o incidentes de seguridad sobre los ciberactivos críticos de las Fuerzas Militares y proyectar su área de cobertura a las infraestructuras críticas de Colombia, incrementar los esfuerzos orientados a elevar los niveles de Ciberdefensa

REACTIVOS	PROACTIVOS	CALIDAD DE LA SEGURIDAD
Alertas y Advertencias	**Anuncios**	**Sensibilización**
Gestión de Incidentes • Análisis de Incidentes • Apoyo a la respuesta a Incidentes • Coordinación de la respuesta a incidentes		
Análisis de Vulnerabilidades		

GESTIÓN EN TIEMPO REAL

- Gestión de Eventos de Seguridad de la Información
- Respuesta en línea a incidentes de Ciberseguridad Centro de Operaciones de Seguridad (SOC)
- Visibilidad y Análisis de Tráfico en Tiempo Real
- Protección de Bases de Datos
- Protección de Portales Web
- Implementación de Esquema de Protección de intrusos
- Análisis de Vulnerabilidades
- Análisis Forense
- Análisis de Malware

ESTRATEGIA DE PROTECCIÓN Y DEFENSA A LA ICCN

Mecanismos de coordinación para la infraestructura crítica cibernética

Centro Operaciones Cibernéticas Conjunto

Políticas Nacionales CONPES 3701 y CONPES 3854 Comisión Nacional Digital

Formación CiberComandos

Convenios y Planes Interinstitucionales

Proyecto: Centro nacional para la Protección y defensa de la IC en Colombia

Iniciativa de Ley para Asuntos del Ciberespacio

Ejercicios de Simulación y Entrenamiento

Plan Nacional para Protección y Defensa de la ICCN

Actualización Periódica Catálogo de ICCN

GESTIÓN 2016

Proceso metodológico y Articulado

- **Acción Unificada -Articulada**
- **Trabajo interinstucional e intersectorial**

1. DEFINIR LÍDERES SECTORIALES — 2013

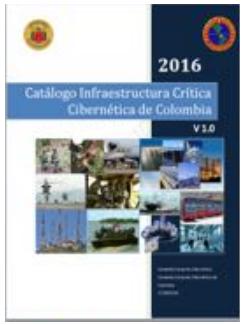
2. EQUIPOS DE TRABAJO SECTORIALES — 2014

3. GUÍA ICC — 2015

4. DOCUMENTO SECTORES ESTRATÉGICOS — 2016

5. CONSOLIDACIÓN INFORMACIÓN

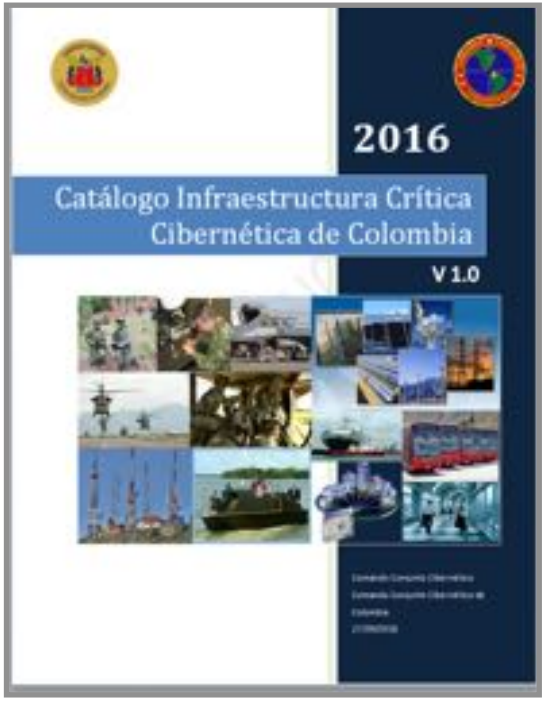
6. CATALOGACIÓN — 2016



INFRAESTRUCTURA CRÍTICA CIBERNÉTICA

¿QUÉ SE HIZO?

Se identificó, clasificó y priorizó la infraestructura crítica cibernética nacional.



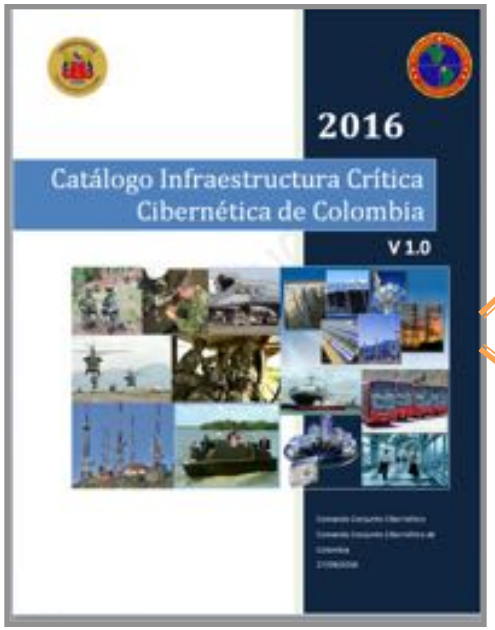
¿QUÉ VIENE?

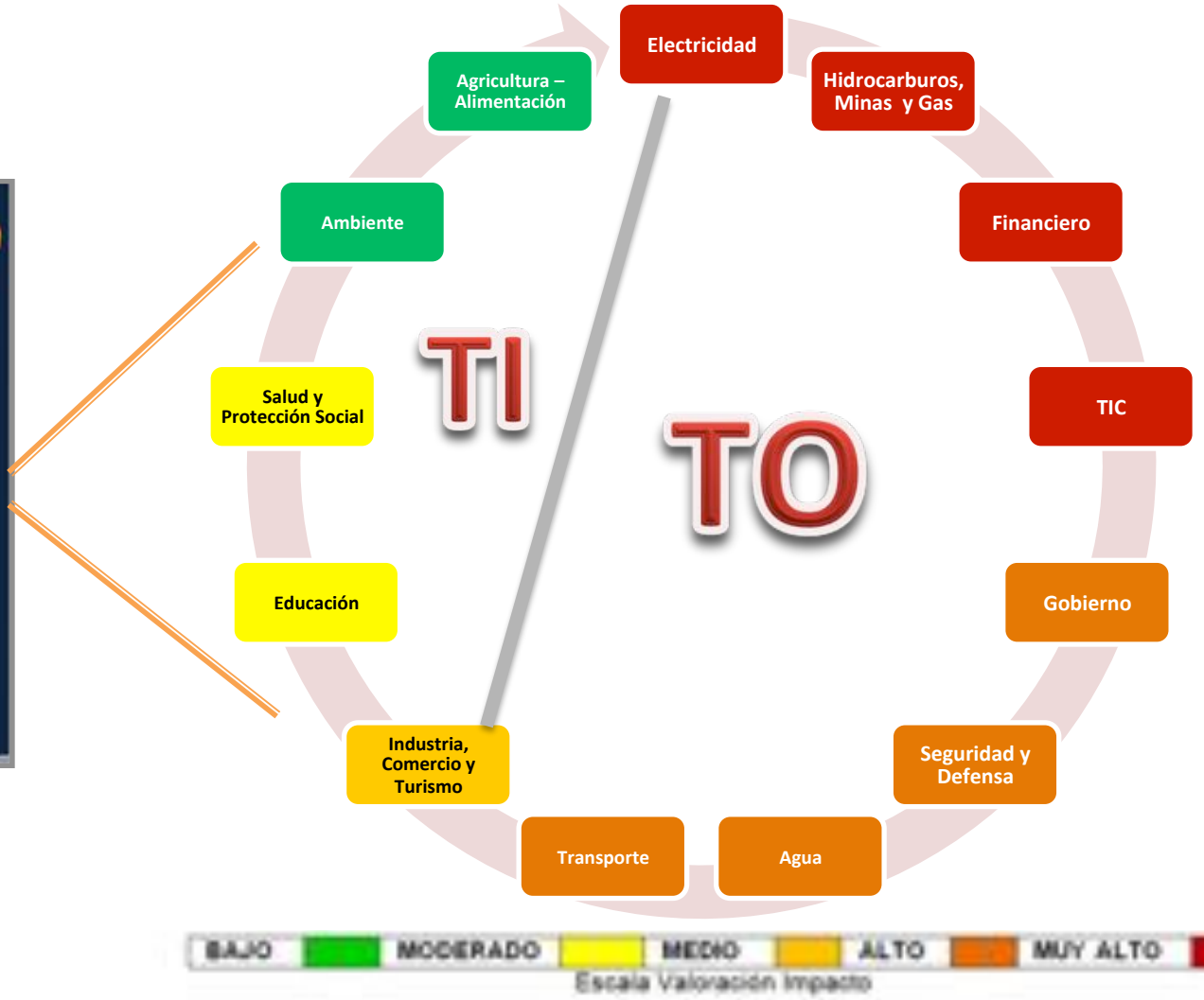
Desarrollo Planes de Protección y Defensa Cibernética

COMANDO CONJUNTO CIBERNÉTICO

Ciberdefensa Nacional a través de operaciones militares cibernéticas

IMPACTO CIBERNÉTICO





METAS 2017:

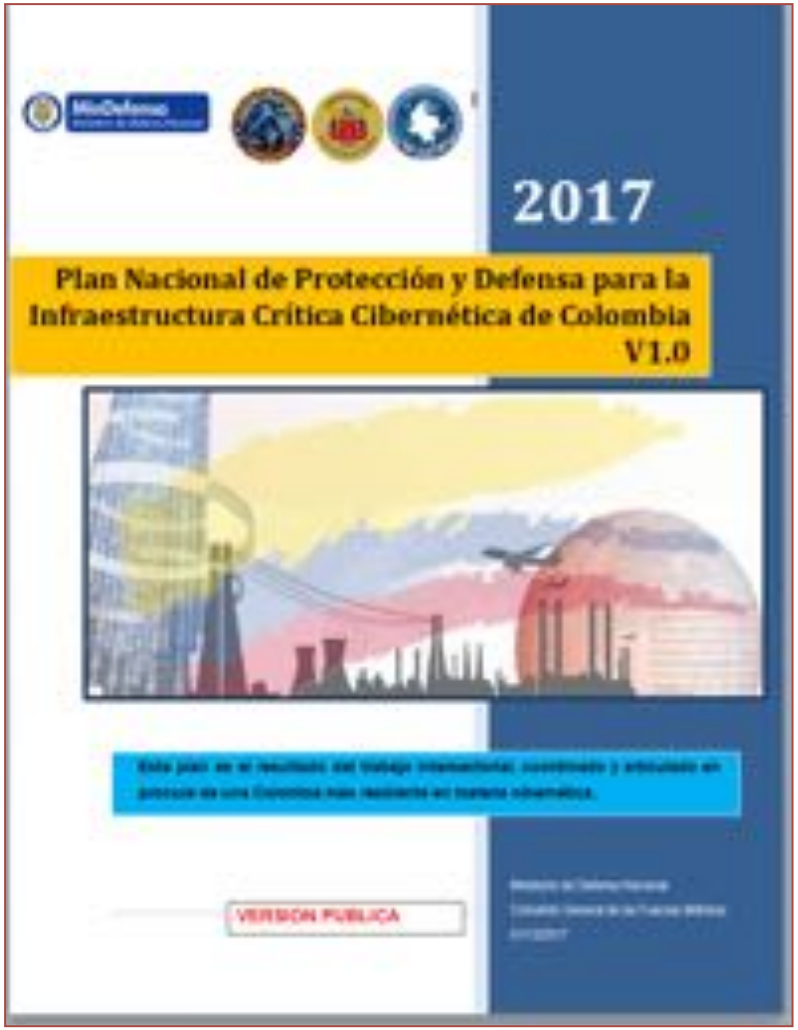
XXXV Reunión de Infraestructura Critica Cibernética, Riesgo operacional y Ciberdefensa
Cámara de Comercio de Bogotá, 31 de Enero de 2017

Plan Nacional protección y defensa de la ICCN

Catálogo ICCN Versión 2

Proyecto Ley Asuntos del Ciberespacio

PNPICCN:


2017
Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia V1.0
VERSION PUBLICA


2017
Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia V1.0
VERSION RESTRINGIDA

OBJETIVOS DEL PNPICCN:

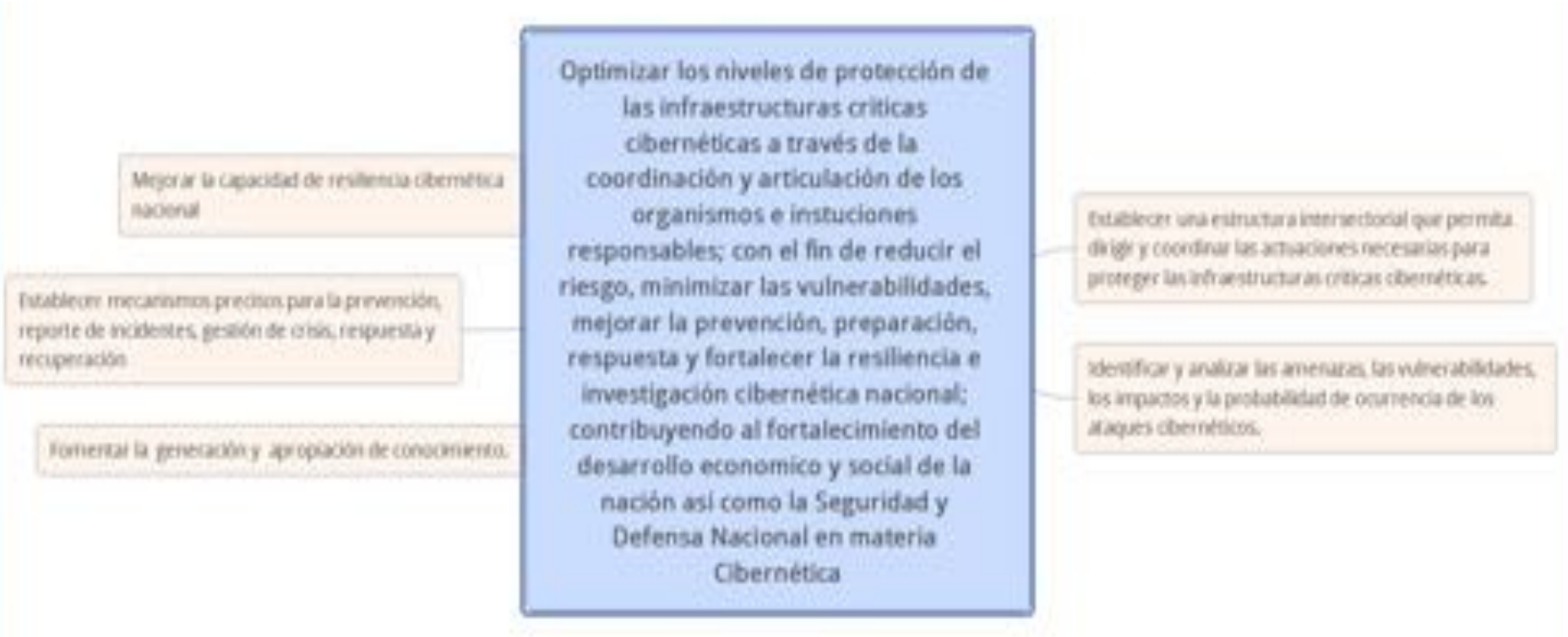
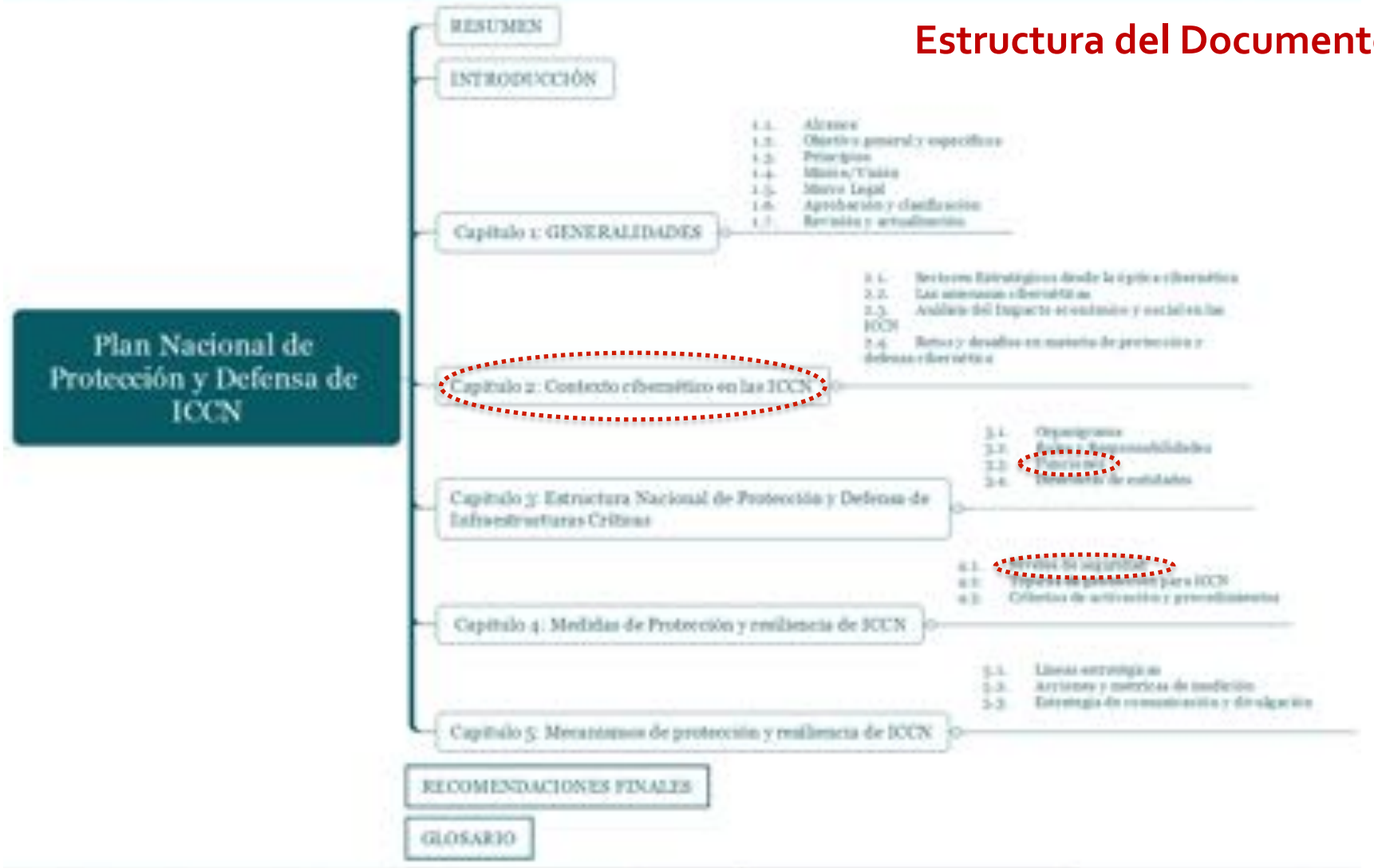


TABLA DE CONTENIDO:

Estructura del Documento



EL SISTEMA:

Sistema Nacional de protección y Defensa de Infraestructuras Críticas Cibernéticas

LÍDERES SECTORIALES:

3.2. Relaciones de Coordinación de Ciberseguridad Y Ciberdefensa

Sector	Líder Sectorial	Ciberseguridad	Ciberdefensa
Alimentación y Agricultura	Ministerio de Agricultura y Desarrollo Rural	COLCERT - CCP - MINTIC	COMANDO CONJUNTO CIBERNÉTICO UNIDADES CIBERNÉTICAS FF.MM.
Agua	Ministerio de Vivienda, Ciudad y Territorio		
Comercio, Industria y Turismo	Ministerio de Comercio, Industria y Turismo		
Seguridad y Defensa	Ministerio de Defensa Nacional		
Educación	Ministerio de Educación Nacional		
Electricidad	Ministerio de Minas y Energía Comisión Nacional de Operación del Sector Eléctrico (CNO)		
Financiero	Ministerio de Hacienda y Crédito Público ASOBANCARIA		
Gobierno	Ministerio de Justicia y del derecho		
Recursos Naturales medio Ambiente	Ministerio de Ambiente y Desarrollo Sostenible		
Recursos Minero Energéticos	Ministerio de Minas y Energía		
Salud y Protección Social	Ministerio de Salud y de la Protección Social		
Tecnologías de la Información y Comunicaciones	Ministerio de las TIC		
Transporte	Ministerio de Transporte		

Sistema Nacional de Alertas Cibernéticas

NORMALIDAD	BAJO	MEDIO	ALTO	EMERGENCIA CIBERNÉTICA
1	2	3	4	5

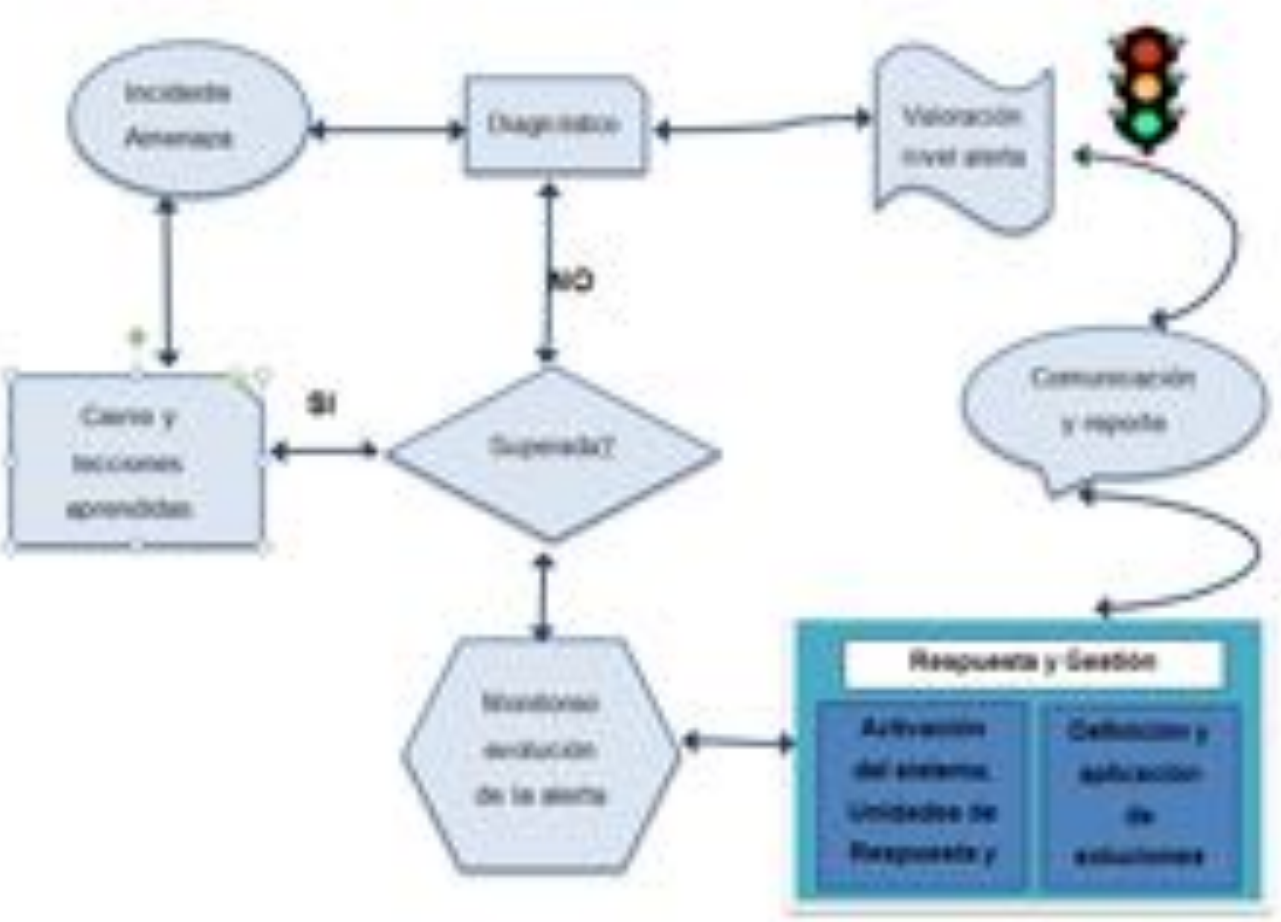
Nivel = I + E+ A

Dónde:

I= Impacto E= Escala

A= Alcance

Proceso para la declaración y atención de una emergencia cibernética



Buenas Practicas para la Protección de ICC

Líneas estratégicas, acciones y métricas

Fortalecer la seguridad de los activos IT/ OT que soportan las Infraestructuras Críticas Cibernéticas Nacionales.

Generar resiliencia, a través del fortalecimiento de las capacidades de respuesta y recuperación ante amenazas cibernéticas y de una adecuada gestión de la resiliencia operativa.

Desarrollar competencias en Ciberseguridad y Ciberdefensa, conocimiento e I+D+i.

Generar normatividad, sinergia Intra-inter sectorial e internacional.

SINERGIA OPERACIONAL

- colCERT
- CCP
- CSIRT Sectoriales
- Sector Privado
- Sector Público
- Sector Inteligencia
- Fiscalía

- Estados Amigos
- Organismos Internacionales
- CERT Internacionales

El Comando Conjunto Cibernético (CCOC) en coordinación con las fuerzas amigas realizará acciones y operaciones cibernéticas conjuntas, coordinadas e interagenciales para proteger la Infraestructura Crítica Cibernética Nacional (ICCN), disputar el control del ciberespacio.


"ESTAMOS
EN EL CORAZÓN DE LOS COLOMBIANOS
AHÍ NOS VAMOS A QUEDAR"

GRACIAS