CONPES “FORTALECIMIENTO Y CONSOLIDACIÓN DE CIBERSEGURIDAD Y CIBERDEFENSA EN COLOMBIA

GOBIERNO DE COLOMBIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

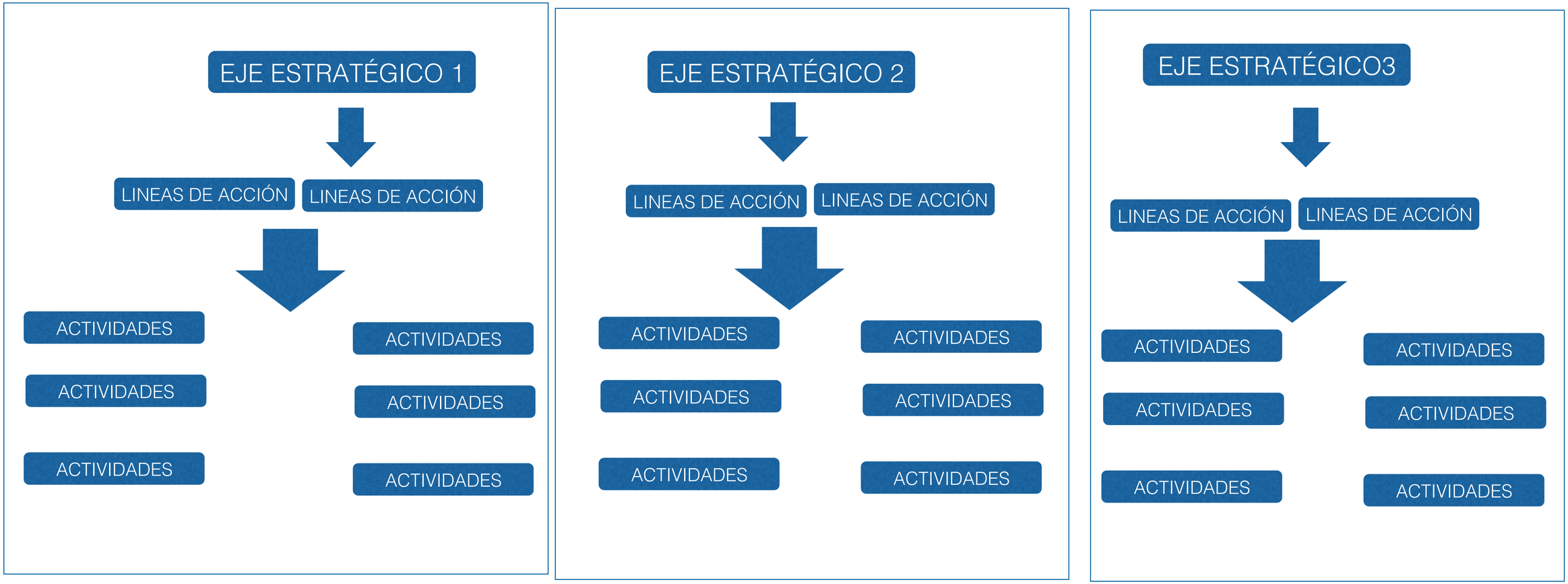
ESTRUCTURA DOCUENTO CONPES

GOBIERNO DE COLOMBIA

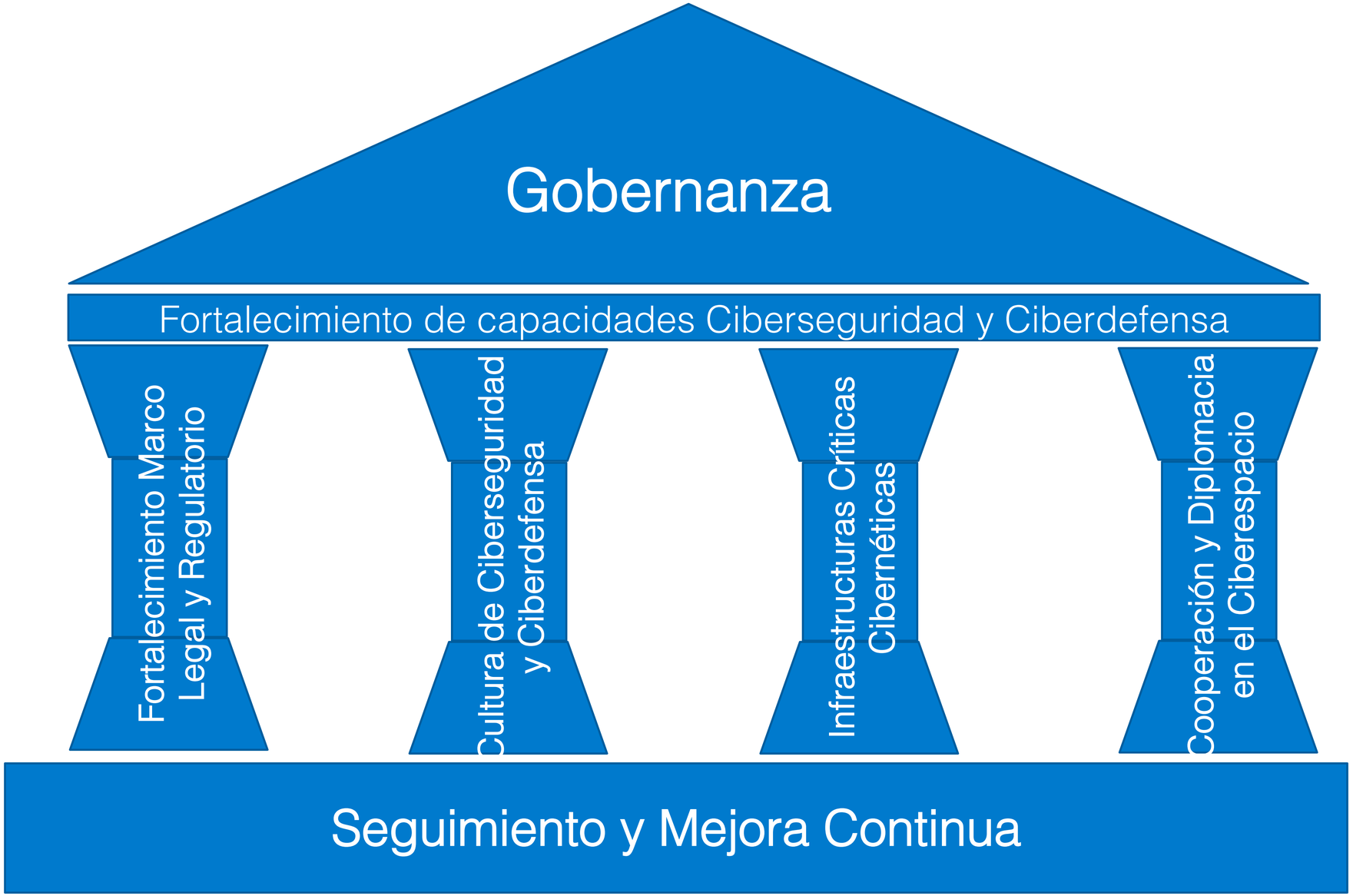
TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

CONPES - ESTRUCTURA

CONPES - METODOLOGÍA



EJES ESTRATÉGICOS



EJE ESTRATEGICO: GOBERNANZA

Alternativas que le permitan al Estado Colombiano, articular y armonizar su orientación, integrar actores y consolidar esfuerzos en aspectos relacionados con la Ciberseguridad y Ciberdefensa.

1. Liderazgo del Gobierno
2. Estructuras organizacionales
3. Coordinación efectiva

Plan de Acción

EJE ESTRATEGICO: DESARROLLO DE CAPACIDADES

Consiste en el fortalecimiento de las instituciones existentes, del recurso humano, los procesos, la tecnología y las habilidades en Ciberseguridad y Ciberdefensa, con un enfoque de coordinación y cooperación para permitir que el país pueda beneficiarse de las ventajas políticas, económicas y sociales que ofrece un ciberespacio seguro y garantizar la Defensa y Seguridad Nacional.

EJE ESTRATEGICO: DESARROLLO DE CAPACIDADES

1. Fortalecimiento de las instituciones responsables de Ciberseguridad y Ciberdefensa
2. Fortalecimiento del Capital Humano
3. Fortalecimiento de las Tecnologías de la Información y Comunicaciones (TIC) para Ciberseguridad y Ciberdefensa.
4. Generación y fortalecimiento de doctrina, procesos y procedimientos de Ciberseguridad y Ciberdefensa.
5. Fortalecimiento de la resiliencia cibernética nacional.
6. Implementación de observatorios y centros de excelencia nacionales en Ciberseguridad y Ciberdefensa.
7. Gestión de incidentes y gestión de crisis.
8. Desarrollo de capacidades criptológicas para la protección y preservación de la información crítica del País.
9. Promover iniciativas para impulsar el desarrollo industrial en Ciberseguridad y Ciberdefensa.

EJE ESTRATEGICO: GENERACIÓN DE UNA CULTURA DE CIBERSEGURIDAD Y CIBERDEFENSA

Incluye la implementación de planes y programas que permitan a los actores y responsables de la Ciberseguridad y Ciberdefensa, prevenir y desarrollar habilidades de respuesta ante amenazas y ataques de naturaleza cibernética mediante el uso de nuevas tecnologías de la información y comunicaciones, procesos y procedimientos establecidos en la materia.

1. Generar conciencia situacional nacional en Ciberseguridad y Ciberdefensa.
2. Fortalecimiento de programas de prevención y capacitación en Ciberseguridad y Ciberdefensa.
3. Fortalecimiento de la educación en Ciberseguridad y Ciberdefensa
4. Investigación, Desarrollo e Innovación en Ciberseguridad y Ciberdefensa

EJE ESTRATEGICO: INFRAESTRUCTURAS CRÍTICAS CIBERNÉTICAS NACIONALES

La protección y defensa de la infraestructura crítica cibernética nacional, se considera fundamental y demanda no solo la participación de los propietarios y/o operadores de dicha infraestructura, sino también requiere el concurso del gobierno, la academia, las Fuerzas Militares, Policía Nacional y de los sectores público y privado.

1. Diseñar e implementar una estructura organizacional para gestión de las infraestructuras críticas cibernéticas nacionales.
2. Desarrollar el catálogo nacional de infraestructura crítica cibernética
3. Identificar, clasificar y priorizar los activos críticos cibernéticos basado en un modelo de gestión de riesgos nacional.
4. Fortalecer la protección y defensa de la infraestructura crítica cibernética nacional.
5. Desarrollar estrategias para la gestión de incidentes y gestión de crisis para infraestructuras críticas cibernéticas nacionales.

EJE ESTRATEGICO: MARCO LEGAL Y REGULATORIO

Las leyes y normativas actuales y futuras así como los convenios internacionales a los cuales la República de Colombia pertenezca o se adhiera, apalancarán y facultarán la ejecución, la legitimidad y el marco procesal requerido, relacionado con Ciberseguridad y Ciberdefensa.

1. Desarrollar mecanismos que permitan fortalecer la armonía legislativa en aspectos relativos a seguridad, privacidad e inteligencia
2. Fortalecimiento del marco legal y regulatorio nacional en materia de Ciberseguridad y Ciberdefensa.
3. Adoptar políticas y lineamientos en materia del Derecho Internacional Humanitario y DD.HH en el ciberespacio.
4. Desarrollo de un marco normativo para la aplicación de capacidades para la protección y defensa de la infraestructura crítica cibernética nacional.
5. Desarrollo de un marco normativo sobre criptología.

EJE ESTRATEGICO: COOPERACIÓN Y DIPLOMACIA EN EL CIBERESPACIO

Permite establecer canales de intercambio de información, recursos y educación en Ciberseguridad y Ciberdefensa con otros países, con organismos nacionales e internacionales, así como fortalecer y estrechar los lazos diplomáticos en relación con el adecuado uso y aprovechamiento del ciberespacio.

1. Desarrollar un marco para el establecimiento de alianzas con partes interesadas.
2. Desarrollar e implementar una agenda estratégica de cooperación nacional.
3. Desarrollar e implementar una agenda estratégica de cooperación internacional.
4. Implementar estrategias para el desarrollo de la Diplomacia en el Ciberespacio.
5. Adhesión a redes de intercambio de información, reporte de incidentes e investigación de ciberseguridad y ciberdefensa.

EJE TRANSVERSAL: SEGUIMIENTO Y MEJORA CONTINUA

Es un eje transversal a los ejes estratégicos que permite realizar monitoreo, evaluación, seguimiento y mejora continua a la implementación del plan de acción, medido con variables de impacto, así como con indicadores de gestión robustos y metas cuantificables.

1. Diseñar e implementar mecanismos de monitoreo y evaluación del plan de acción.
2. Establecer una metodología para garantizar el seguimiento y mejora continua del plan de acción.

PLAN DE ACCIÓN

Infraestructuras Críticas Cibernéticas Nacionales				
ACCIÓN	ENTIDAD	DEPENDENCIA	FECHA INICIO	FECHA FIN
Diseñar e implementar una estructura organizacional para las infraestructuras críticas cibernéticas nacionales.				
Definir roles y responsabilidades de los actores y responsables de la Infraestructura Critica Cibernética Nacional.				
Desarrollar y socializar planes de protección y defensa de la Infraestructura Critica Cibernética Nacional.				
Promover y fomentar la Ciberseguridad de las Infraestructuras críticas cibernéticas				

GRACIAS

GOBIERNO DE COLOMBIA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN