ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
Colombia

KONRAD ADENAUER STIFTUNG

Estrategia de Seguridad para las

REDES DE COMUNICACIÓN NACIONAL Y LA CONECTIVIDAD CON EL CIBERESPACIO

2022 - 2032

Estrategia de Seguridad
para las

REDES DE COMUNICACIÓN NACIONAL Y LA CONECTIVIDAD CON EL CIBERESPACIO

2022 - 2032

Catalogación en la publicación – Escuela Superior de Guerra "General Rafael Reyes Prieto"

Estrategia de seguridad: para las redes de comunicación nacional y la conectividad con el ciberespacio 2022-2032 / Brigadier General Edgar Alexander Salamanca Rodríguez, General (R) Fabricio Cabrera Ortiz, Stefan Reit - Bogotá: Editorial ESDEG, Fundación Konrad Adenauer KAS, 2022.
100 páginas: ilustraciones, fotografías cuadros y gráficas; 24 cm.
Incluye referencias bibliográficas página 98.
ISBN 978-628-95304-0-7
E- ISBN 978-628-95304-1-4
1. Ciberespacio -- Sistemas de comunicación -- Colombia 2. Sistemas de telecomunicación -- Colombia 3. Ingeniería de sistemas -- Colombia 4. Colombia -- Sistemas de comunicación i. Salamanca Rodríguez, Edgar Alexander, Brigadier General (editor - autor) ii. Cabrera Ortiz, Fabricio, Brigadier General (R) (editor - autor) iii. Reith, Stefan, (editora - autora) iv. Salgado Romero, Luis Fernando, Coronel, (autor) v. Cotua Muñoz, Yor William, Coronel, (autor) vi. Forero Camacho, Danysh Adey, Coronel, (autor) vii. Souza Lima, Leonardo Freitas de, Coronel, (autor) viii. Colombia. Escuela Superior de Guerra. ESDEG. Departamento Curso de Altos Estudios Militares y Curso Integral de Defensa Nacional (CAEM – CIDENAL) ix. Fundación Konrad Adenauer, KAS

HM851 E88 2022 Registro Catálogo SIBFuP 991238910607231
303.4833 -- 23

Archivo descargable en formato MARC en: https://tinyurl.com/esdeg991238910607231

Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio 2022 - 2032
Primera edición, 2022

Editores
Brigadier General Edgar Alexander Salamanca Rodríguez
Subdirector Escuela Superior de Guerra
Brigadier General (R) Fabricio Cabrera Ortiz
Jefe Departamento CAEM - CIDENAL
Stefan Reith
Representante Colombia Fundación Konrad Adenauer, KAS

Autores
Curso de Altos Estudios Militares No. 63
CR (EJC) Luis Fernando Salgado Romero
CR (EJC) Yor William Cotua Muñoz
CR (FAC) Danysh Adey Forero Camacho
CR (BRASIL) Leonardo Freitas de Souza Lima

Estudiantes Curso Integral de Defensa Nacional No. 49
CR (PNC) Faxir Ramírez Horta
CR (PNC) Olga Patricia Salazar Sánchez
Santiago Barbosa Delgado
Camilo Fernández de Soto Camacho
Lizbet Karina Navarro Santamaría
Mario Pardo Bayona
Claudia Bibiana Ramírez Jaramillo
Carlos Andrés Ríos Puerta
Karen Rojas Ramos
Javier Augusto Sarmiento Olarte
José Luis Valderrama Gutiérrez

Corrección de estilo
Magda Livy Castellanos Muñoz

Diagramación y diseño gráfico
Raquel Arianne Alvarado Candela

Imágenes portada y contraportada
Revista Aeronaútica Fuerza Aérea Colombiana
Policía Nacional de Colombia - MinTIC

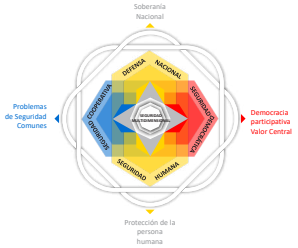
2022 Escuela Superior de Guerra
"General Rafael Reyes Prieto" - ESDEG
Departamento Curso de Altos Estudios Militares y Curso Integral de Defensa Nacional (CAEM – CIDENAL)
Carrera 11 No. 102-50 Bogotá D.C., Colombia
(+57) 601 620 4066
www.esdeglibros.edu.co

2022 Fundación Konrad Adenauer, KAS, Colombia
Calle 93B No. 18-12, Piso 7 Bogotá, D.C., Colombia
(+57) 601 743 0947
www.kas.de/web/kolumbien

Libro electrónico publicado a través de la plataforma Open Monograph Press.
Tiraje de 400 ejemplares
Opciones Gráficas Editores Ltda.
Impreso en Colombia - *Printed in Colombia*

ISBN impreso: 978-628-95304-0-7
ISBN digital: 978-628-95304-1-4
https://doi.org/10.25062/9786289530414

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa la posición oficial ni institucional de la Escuela Superior de Guerra "General Rafael Reyes Prieto" y de la Fundación Konrad Adenauer, KAS.



CONTENIDO

RESUMEN EJECUTIVO

La Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio que aquí se presenta, tiene como propósito plantear en un contexto estratégico los objetivos, líneas de acción y actividades que deben gestionar los altos dirigentes del Estado para neutralizar y/o mitigar los riesgos, amenazas y desafíos que pueden afectar el normal funcionamiento del país, su interrelación con otras naciones y organismos internacionales de carácter multilateral, así como su capacidad para responder de manera sincronizada y articulada ante situaciones de crisis que se puedan suscitar un ambiente con volatilidad, incertidumbre, condiciones de complejidad y ambigüedad.

Por lo anterior, los contenidos están redactados en un lenguaje no técnico, y fácil de entender para cualquier ciudadano, principalmente porque la publicación está dirigida a quienes ejercen el liderazgo civil, militar y policial en todos los niveles de la administración territorial del país, en donde desempeñan cargos en los ámbitos estratégico, operacional o táctico y se encargan de planear y gestionar de acuerdo a sus áreas de responsabilidad, diversos medios con el fin de asignar actividades que originen un trabajo sinérgico entre los actores que integran las entidades nacionales e internacionales con naturaleza pública o privadas del orden nacional e internacional.

A su vez, se constituye como una herramienta que complementa los planes de desarrollo para evitar la exclusión de otros aspectos que deban considerarse al momento de formular e implementar planes de acción y proyectos para optimizar las proyecciones y resultados a partir de su aplicación.

El listado de riesgos, amenazas y desafíos abordados de manera muy general, fueron utilizados como insumo para el planteamiento de la estrategia con la cual se pretende neutralizar y/o mitigar los efectos no deseados en caso de que algunos de ellos se materialicen. De igual forma, contribuye con la generación de un análisis reflexivo respecto a aspectos específicos que los líderes responsables de gestionar los planes de acción deben tener en cuenta para conseguir el aumento de las coberturas de comunicaciones y conectividad con el ciberespacio en las áreas de responsabilidad territorial asignadas, anticipando el mantenimiento de equipos, su actualización, la redundancia, complementariedad necesaria, la renovación y en general las acciones que conlleven a garantizar la capacidad de la nación para transmitir y recibir voz y datos; así como para interconectarse a través del espacio y ciberespacio.

En consecuencia, el estado final deseado para la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio, apunta a que el país disponga de las capacidades tecnológicas, multiespectrales y multidominio necesarias, ajustadas al adelanto de las tecnologías de la información y comunicaciones; caracterizándolas como robustas, redundantes, complementarias, protegidas de amenazas, los riesgos, amenazas y desafíos antrópicos y/o naturales, en las que se cuente con una recuperación del servicio eficiente ante una afectación, con efectividad en los procesos de recepción y transmisión confiable voz y datos, así como la interrelación e interconexión a través del espacio y ciberespacio a nivel nacional, regional, hemisférico y global.

En la parte final, se presentan algunas consideraciones que deben ser tenidas en cuenta por quienes sean responsables de aportar en la construcción del futuro deseado para el país.

INTRODUCCIÓN

La comunicación ha sido esencial en los procesos evolutivos y para la historia de la humanidad, su aporte sirvió para que los líderes de las tribus primitivas, de clanes y nacientes sociedades que posteriormente se convirtieron en Estados nación, pudieran ejercer el dominio y la soberanía sobre sus territorios. De igual manera, es adecuado afirmar que la comunicación ha facilitado el entendimiento e interrelación entre grupos humanos contribuyendo para que alcancen sus objetivos conforme a los intereses del momento histórico y el logro del bienestar general.

En coherencia con lo descrito, es importante indicar que los avances tecnológicos e industriales sumados a las circunstancias propias del momento llevaron al crecimiento económico y exponencial de algunas naciones, las cuales se fortalecieron en diversos campos hasta convertirse en potencias dentro del orden mundial. Las máquinas de vapor, la energía hidráulica y la mecanización de procesos con los cuales se amplió la posibilidad de generar recursos económicos desde fuentes diferentes a la agricultura, fomentó la producción en las nacientes empresas, lo que estableció las bases para que a mediados del siglo XVIII se generara la Primera Revolución Industrial.

> Son visibles necesidades frente al fortalecimiento y masificación del conocimiento, como medio para la potenciación de las competencias del talento humano frente al uso de herramientas digitales, las técnicas de minería y análisis de datos, la programación y la inteligencia artificial.

El telégrafo, el automóvil, el aeroplano, las nuevas fuentes de energía y en general la aparición de otras tecnologías propiciaron cambios en los procesos empresariales, científicos y en la sociedad,

permitieron acelerar los tiempos y cantidades de producción, siendo necesario ampliar los conceptos relativos de competitividad que se fueron consolidado durante la denominada Segunda Revolución Industrial alrededor del año 1870 (de Motes, 1992).

Posteriormente, las tecnologías de la información y las comunicaciones, las redes eléctricas inteligentes y el uso de energías renovables, permitieron una mayor eficiencia mediante la automatización en la producción, lo cual motivó la clasificación de la denominada Tercera Revolución Industrial a mediados del siglo XX.

Con la Cuarta Revolución Industrial se manifiesta el dinamismo de las tecnologías y de la mixtura de los sistemas digitales y físicos; por lo cual, son visibles necesidades frente al fortalecimiento y masificación del conocimiento, como medio para la potenciación de las competencias del talento humano frente al uso de herramientas digitales, las técnicas de minería y análisis de datos, la programación y la inteligencia artificial, entre otros aspectos relevantes que aportarán a la sociedad para superar los retos actuales y futuros de la mejor manera posible.

Las denominadas guerras de quinta generación (G5G) que se desarrollan de forma simultánea en los ámbitos terrestres, marítimos, fluviales, aéreos, espaciales, ciberespaciales y cognitivos involucran actores ubicados en cualquier parte del planeta, ya que gracias a las Tecnologías de la Información y las Comunicaciones, además de las facilidades del ciberespacio, el teatro de la guerra se ha desarrollado superando la zona de confrontación bélica sobre el terreno, en el replanteamiento de las estrategias de Defensa y Seguridad de los Estados.

El fenómeno de la globalización se ha fortalecido gracias a las tecnologías digitales e informáticas permitiendo construir puentes virtuales a través del ciberespacio en todo el planeta, acercando territorios físicamente distantes entre sí. El alcance del mensaje transmitido trasciende las fronteras y se puede difundir de manera inmediata a casi todo planeta en donde existan los medios para establecer la comunicación, e incluso en el espacio exterior (aunque

aún no exista evidencia de que se haya recibido respuesta alguna), para lo cual, contar con una red de comunicaciones confiable, moderna, segura es indispensable si se quiere transmitir de forma exitosa mensajes de voz y datos en tiempo real.

En el mismo sentido, es importante disponer de medios tecnológicamente avanzados, apropiados de acuerdo al mensaje que se quiere transmitir, las condiciones propias del terreno, la geografía, ambiente y capacidades previamente instaladas; a fin de ejercer el dominio y mantener la superioridad en este ambiente, en la consecución de comunicaciones positivas y la difusión de un mensaje claro, preciso, oportuno y seguro respondiendo a los requerimientos del liderazgo civil, militar o población en general; para que las personas ejecuten las actividades propias que contribuyan a su bienestar y crecimiento del Estado en un entorno seguro.

Por lo tanto, es fundamental identificar los principales sistemas en uso y los de soporte que contribuyen al funcionamiento y conectividad de los medios tecnológicos empleados para este fin, así como sus riesgos, amenazas y desafíos en la generación de un diagnóstico preliminar que contribuya a proponer las acciones necesarias para evitar su afectación por causas antrópicas o fenómenos naturales en la provisión de los servicios de comunicación y transmisión de voz y datos necesarios para el país en el ámbito interno y para conectarse con el mundo de manera permanente.

Hoy, asegurar la conectividad e identificar claramente las redes de comunicación con las que cuenta el país para ejercer su soberanía, desenvolverse en el diario vivir y proyectarse hacia un futuro deseado, se convierte en una prioridad estratégica que va a posibilitar que se conserve la superioridad en los ámbitos terrestres, marítimos, fluviales, aéreos, espaciales, ciberespaciales y cognitivos.

En concordancia con lo expuesto y, teniendo en cuenta la infraestructura referente a las tecnologías de la información y comunicaciones existente en el país, el dinamismo tecnológico actual, la necesidad de gobernanza, los intereses nacionales,

el posicionamiento regional, hemisférico y global alcanzado, la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio se enfoca en garantizar la capacidad de la nación para transmitir y recibir voz y datos, así como para interconectarse a través del espacio y ciberespacio, al igual que proteger de amenazas antrópicas o naturales las redes usadas para transmitir y recibir voz y datos de la nación (Vargas, 2002).

PROPÓSITO

Plantear en un contexto estratégico, los objetivos, líneas de acción y actividades que se deben gestionar por parte de los altos dirigentes del Estado para neutralizar y mitigar las riesgos, amenazas y desafíos que pueden afectar el normal funcionamiento del país, su interrelacionamiento con otras naciones y organismos internacionales de carácter multilateral, así como su capacidad para responder de manera sincronizada y articulada ante crisis que puedan generarse en un ambiente volátil, marcado por la incertidumbre, complejo y con ambigüedad.

ESTADO FINAL DESEADO

Tener un país con las capacidades tecnológicas necesarias, multiespectrales y multidominio, actualizadas de conformidad con los momentos evolutivos propios de las tecnologías de la información y comunicaciones; robustas, redundantes y complementarias, preservadas de riesgos, amenazas y desafíos antrópicas o naturales, de rápida recuperación del servicio ante una afectación, que permitan en todo momento de manera confiable y segura, transmitir y recibir voz y datos, así como la interrelación e interconexión a través del espacio y ciberespacio a nivel nacional, regional, hemisférico y global.

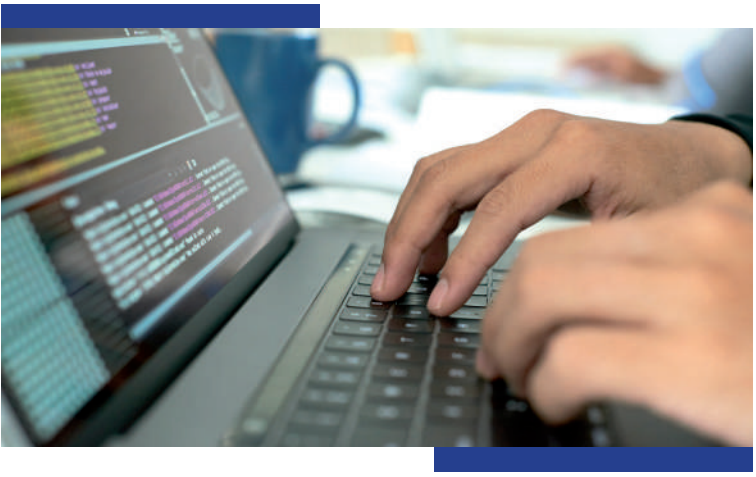
CONTEXTO ESTRATÉGICO

CAPÍTULO 1

CONTEXTO ESTRATÉGICO

1.1 Generalidades

Las migraciones desordenadas que se presentan en América Latina y que se originan diversos factores como crisis económicas, desastres naturales, inestabilidad política en los países de la región, entre otras causas, son un factor sustancial para tener en cuenta en los procesos de planificación gubernamental. Las infraestructuras de apoyo presentes en una región determinada pueden ser objeto de requerimientos inesperados, saturando las capacidades considerando factores asociados al bajo nivel de calidad para los servicios públicos disponibles e incluso, en el colapso momentáneo o parálisis en la provisión de estos.



Teniendo en cuenta la definición vista en el material de estudio titulado La Guerra en la Historia de la Humanidad (s.f.), citada por Ramírez et al. (2017), en la que indica que "la guerra es un estado de conflicto colectivo y organizado, que puede desarrollarse a través de hostilidades violenta y no violentas" (p.152) y que para el caso de las guerras de quinta generación "G5G" pueden extender el teatro de las confrontaciones más allá del espacio geográfico donde se desarrollan, es posible afirmar que se presenta una oportunidad mayor para la profundización del conflicto, debido a la disponibilidad de medios tecnológicos y capacidades del espacio y ciberespacio asequibles a la mayoría de la población, admitiendo la participación a individuos o colectivos con intereses diferentes a los que motivaron el enfrentamiento entre los actores en guerra.

En ese contexto, se hace necesario reflexionar frente al impacto producido por las transformaciones tecnológicas en la sociedad, considerando las facilidades de acceso a datos e información ilimitada que estas ofrecen las 24 horas del día desde cualquier ubicación y a través de diversos medios como computadores u otros dispositivos inteligentes que,

de acuerdo a su desarrollo, incluyen aplicaciones y herramientas con las que se difunden contenidos que permiten influir de manera directa e indirecta, consciente o inconsciente en el pensamiento y la actuación de los seres humanos individual y/o colectivamente (Álvarez et al, 2017).

En un mundo cada vez más interconectado, las situaciones propias de los ambientes "Volátiles, Inciertos, Complejos y Ambiguos" (VICA) son más frecuentes y junto con los potenciales desastres generados por el cambio climático, dinámicas físicas del planeta o propias de la meteorología espacial; exigen que se aseguren las comunicaciones efectivas en tiempos de paz, guerra o crisis, para asegurar la supervivencia de la nación y contribuir a la disminución del sufrimiento humano, preservar la vida, proteger la propiedad privada, mitigar los daños sufridos y restituir las condiciones para tener una vida normal a la brevedad posible.

Asegurar la conectividad para que las Tecnologías de la Información y las Comunicaciones de Colombia funcionen y se articulen de la mejor manera en el entorno local y global es vital; esto implica tener presentes dos grandes grupos de amenazas que podrían generar afectación a la comunicación y transmisión de voz y datos. La primera, denominada como antrópica, se genera por actores contrarios a los intereses del Estado o que pretenden vulnerar la democracia, el Estado de derecho, el respeto a los Derechos Humanos; la segunda, es la amenaza causada por fenómenos naturales de diferente índole, entre las que se observan terremotos, inundaciones, tormentas, tormentas solares.

Entre tanto, diferentes fenómenos contemporáneos como como los ciberataques, la militarización del espacio, el cambio climático, catástrofes meteorológicas, la migración descontrolada, pandemias (COVID-19), desequilibrios demográficos, que se suman a las amenazas hibridas y generan un impacto notable en aspectos como la estabilidad social, la seguridad internacional y el bienestar de los ciudadanos.

Exigen que se aseguren las comunicaciones efectivas en tiempos de paz, guerra o crisis, para asegurar la supervivencia de la nación y contribuir a la disminución del sufrimiento humano, preservar la vida, proteger la propiedad privada, mitigar los daños sufridos y restituir las condiciones para tener una vida normal a la brevedad posible.

El mundo está interconectado y a partir de esta situación se han desarrollado una serie de capacidades tecnológicas a través de diferentes medios y dispositivos que facilitan el establecimiento de ese vínculo entre personas, organizaciones, países, instituciones, etc., incidiendo en la evolución, el desarrollo, la productividad y todo lo que concierne a las actividades del hombre en la actualidad, haciendo que para ninguna sociedad sea aceptable vivir sin redes de comunicación altamente eficaces; ya que las ventajas proporcionadas por las redes de comunicación se consolidan como un activo estratégico que es indispensable proteger.

Los analistas y estrategas dirigen su esfuerzo a crear herramientas que aporten para eliminar las amenazas contra estos activos. Día a día se presentan diferentes enfoques en temas de seguridad relacionados con la conectividad y las redes, por lo que la implementación y la estrategia de la seguridad en este tema se asocia al sistema internacional para conseguir la articulación que requiere un mundo globalizado ante esas amenazas, implicando el desarrollo continuo de mecanismos de innovación dirigidos a fortalecer los temas de seguridad en las redes de comunicación conforme a la evolución de estas tecnologías.

Las redes de apoyo a la infraestructura crítica o los servicios públicos deben ampliarse para satisfacer rápidamente un aumento de la demanda local; exigiendo la creación de planes de contingencia que impliquen la protección física de estas instalaciones e infraestructura, desarrollando capacidades suficientes para realizar reparaciones y mantenimientos de manera rápida, incluyendo la articulación permanente entre agencias gubernamentales responsables de esta área y las principales empresas del sector a fin de crear una sinergia para la integración efectiva de las capacidades en la contención de las posibles amenazas.

1.2 Plataforma estratégica del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

Colombia no ha sido menor a los retos en materia de tecnología, redes y conectividad evolucionando continuamente en esta área. Es así como desde la Carta magna de 1991 se garantizó a través de los artículos 75 y 76 "la igualdad de oportunidades y el pluralismo informativo" (Constitución Política de Colombia, 1991), por lo que se creó un Ministerio de Tecnologías de la información TICS del cual hacen parte dos viceministerios: el viceministerio de Conectividad y Digitalización, que cuenta con dos direcciones (Infraestructura e Industria de las comunicaciones) y el viceministerio de Transformación Digital, que tiene tres direcciones (Gobierno digital, Apropiación TIC y Economía digital).

De acuerdo con "la Ley 1341 de 2009, o Ley de TIC, el Ministerio de Tecnologías de la Información y la Comunicaciones

> es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones" (MinTIC, 2022). Su misión principal es la de "incrementar y facilitar el acceso de todos los habitantes del territorio nacional a las Tecnologías de la Información y las Comunicaciones y a sus beneficios" (Ley 1341 de 2009).

A su vez, mencionada Ley, indica que hace parte de

> los objetivos del Ministerio de las Tecnologías de la Información y las Comunicaciones "diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones en el país" (Ley 1341 de 2009, art. 17).

1.2.1 Objetivos del MinTIC

Según lo dispuesto en el Decreto 1414 (2017), los objetivos de este Ministerio son:

Figura 1. Descripción de los objetivos del MinTIC

Fuente: MinTIC, 2022

1.3 Políticas y lineamientos del Ministerio de Defensa Nacional relativas a las redes de comunicación nacional y la conectividad con el ciberespacio

El Ministerio de Defensa Nacional es el encargado de prestar especial atención a la mejora de las capacidades tecnológicas y de conectividad para afrontar crisis en un trabajo articulado con el Ministerio de Tecnologías de la Información y las Comunicaciones, este último, estableciéndose como órgano de apoyo, debe propender por la integración y disposición de los sistemas de energía y redes de transporte de la comunicación a nivel nacional en caso de crisis si están en riesgo los intereses vitales del Estado.

> Garantice alternancia en la infraestructura de las redes de comunicación y sistemas de energía en casos de amenaza transitoria o permanente, interna o externa, que pueda afectar los intereses vitales o estratégicos, de tal forma que garantice la conectividad y redes de transporte permanentemente con previa coordinación, a partir de la implementación de protocolos estrictos de seguridad.

Lo anterior, en el objetivo de establecer un sistema de conectividad y redes que puedan ser complementarias entre los dos ministerios; implementando un sistema robusto que garantice alternancia en la infraestructura de las redes de comunicación y sistemas de energía en casos de amenaza transitoria o permanente, interna o externa, que pueda afectar los intereses vitales o estratégicos, de tal forma que garantice la conectividad y redes de transporte permanentemente con previa coordinación, a partir de la implementación de protocolos estrictos de seguridad.

1.4 Lineamientos y capacidades del Comando General de las Fuerzas Militares y su articulación con el Ejército Nacional, la Armada de Colombia, la Fuerza Aérea Colombiana y la Policía Nacional.

Las Fuerzas Militares y la Policía Nacional conservarán las capacidades requeridas para actuar de manera autónoma cuando fuere necesario, en coherencia con su objetivo de asegurar la soberanía e intereses nacionales en materia de conectividad y redes de comunicación.

El Comando General de las Fuerzas Militares (COGFM), en cabeza del Departamento Conjunto de Comunicaciones (CGDJ6), consciente de su misión de "asesorar y planear el direccionamiento estratégico por capacidades en cualquier escenario de las tecnologías de la información, para la integración e interoperabilidad en las

Fuerzas Militares" (Comando General de las Fuerzas Militares, 2019), a través de la estrategia de "Gobierno Digital", se ha encargado de fortalecer al COGFM y a las diferentes Fuerzas, mediante la integración de capacidades de soporte y operacionales propias de la Red Integrada de Comunicaciones (RIC) y las tecnologías de la información del departamento.

1.4.1 Plan Estratégico de Tecnologías de Información (PETI) del COGFM, líneas de acción y perspectivas

Con base en lo descrito y en cumplimiento de la misión institucional, el CGDJ6, elabora el PETI institucional para el COGFM, siendo este el documento que reúne los objetivos estratégicos institucionales, que son sumados a los lineamientos de la última versión del Modelo de Planeación y Desarrollo de Capacidades de la Fuerza Pública y otras directrices emitidas a través del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), el Ministerio de Defensa Nacional (MDN) y demás entes gubernamentales (Ministerio de Defensa Nacional, 2018).

El PETI plantea el cambio de paradigmas sobre las tecnologías en las Fuerzas Militares y el COGFM, en la implementación de nuevas perspectivas retadoras, a través de la definición de rupturas estratégicas relacionadas con el cierre de las brechas que se definen en las capacidades priorizadas para el área funcional TIC (Ministerio de Defensa Nacional, 2019).

Basado en los lineamientos del PETI sectorial y la identificación de necesidades expuestas por las direcciones que conforman el CGDJ6, el PETI institucional se plantean seis líneas de acción que sirven como base para direccionar el trabajo relacionado con las TIC liderado por el COGFM como entidad responsable a nivel institucional (Ministerio de Defensa Nacional, 2019, p.6):

Figura 2. Líneas de Acción del PETI

Fuente: Comando General de las Fuerzas Militares, 2019 - 2022

De la misma forma, el Plan Estratégico de Tecnologías de Información (PETI) del COGFM presenta una estrategia enfocada en las TIC, la cual, establece cuatro perspectivas estratégicas que apoyan las acciones encaminadas al logro de las seis líneas de acción determinadas para ello. Estas perspectivas son (Ministerio de Defensa Nacional, 2019, p. 6):

1. Gestión de competencias de TIC.
2. Gestión de procesos y proyectos de TIC
3. Ofrecer servicios efectivos de TIC para las Fuerzas Militares.
4. Aporte y valor agregado de las inversiones en TIC para las diferentes Fuerzas.

> El PETI plantea el cambio de paradigmas sobre las tecnologías en las Fuerzas Militares y el COGFM, en la adopción de nuevas perspectivas retadoras, a través de la definición de rupturas estratégicas relacionadas con el cierre de las brechas que se definen en las capacidades priorizadas para el área funcional TIC (Ministerio de Defensa Nacional, 2019).

Figura 3. Estructura organizacional CGDJ6

Nota. La figura expone la estructura del CGDJ6 conforme a lo definido en la resolución ministerial 3877 del 6 de junio de 2018 y la disposición 013 del 23 de abril de 2018. Fuente. Ministerio de Defensa Nacional (2018).

El direccionamiento estratégico de las tecnologías de la información y de las comunicaciones en el COGFM está a cargo del jefe del Departamento Conjunto de Comunicaciones (CGDJ6), a través de sus cuatro Direcciones: Dirección de Planificación en Comunicaciones y TI (DIPCO), Dirección de Proyectos y Gestión TIC (DIPGE), Dirección de Tecnologías de la Información (DITIN) y Dirección Administrativa de Comunicaciones y TI (DIACO).

Desde su función, asesora y planea la forma como se direccionará desde el enfoque estratégico por capacidades para cualquier escenario en el que estén implicadas las comunicaciones y tecnologías de la información, en la consecución de la integración e interoperabilidad en las Fuerzas Militares (Comando General de las Fuerzas Militares, 2019). Trabaja en conjunto con el Centro de Comunicaciones Conjunto (CECCO), el cual gestiona las capacidades operacionales de comunicaciones del COGFM, que a su vez, suministra servicios a través de la RIC y proporciona conectividad e interoperabilidad a las diferentes plataformas tecnológicas a nivel estratégico en la ejecución de las operaciones conjuntas, coordinadas, interinstitucionales y combinadas (OCCIC), además lidera la inserción de los estándares de las Tecnologías de la Información y Comunicación (TIC) en el COGFM, propone acciones para la consolidación y capacitación tecnológica en la institución, y también, coordina la inclusión y práctica de las políticas y directrices relacionadas con el tema TIC, las cuales son emitidas por el Gobierno nacional (Ministerio de Defensa Nacional, 2018).

1.5 Lineamientos y capacidades de la Policía Nacional y su articulación con las FF.MM. de la República de Colombia

Oficinas asesoras - Telemática - Policía Nacional

1.5.1 Misión y visión de la oficina de Telemática de la Policía Nacional

De acuerdo con la Policía Nacional, la misión de la Oficina de Telemática es:

> asesorar y promover el desarrollo tecnológico de la institución en las áreas de informática y telecomunicaciones a través de la investigación, implementación, administración y soporte, con el fin de estandarizar los procedimientos e innovar la infraestructura tecnológica para apoyar la gestión policial. (Oficina de Tecnologías de la Información y las Comunicaciones, 2022)

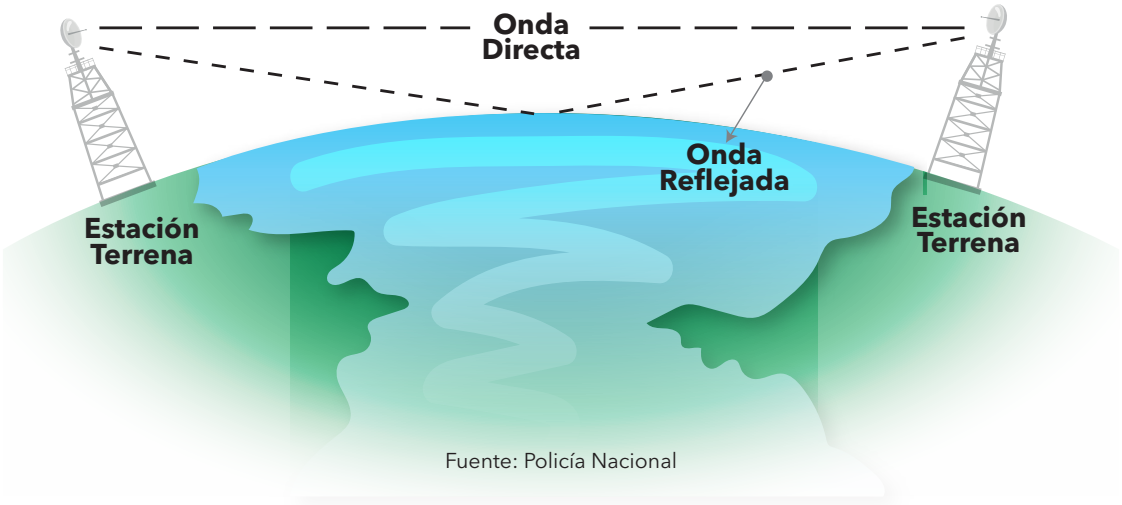
Así mismo, en la visión formulada se proyecta una Policía Nacional que se considere como

> referente tecnológico a nivel local y global, resultado de una gestión eficiente de las Tecnologías de la Información y las Comunicaciones, que transforma los procesos de negocio y brinda servicios digitales con altos estándares de calidad y seguridad para contribuir a la construcción de un Estado abierto, eficiente, transparente y participativo. (Dirección General - Oficina de Telemática, 2019)

Figura 4. Parámetros del funcionamiento de la red de comunicaciones de la Policía Nacional

Fuente: Policía Nacional

Figura 5. Enlace de Microondas de Línea de Vista

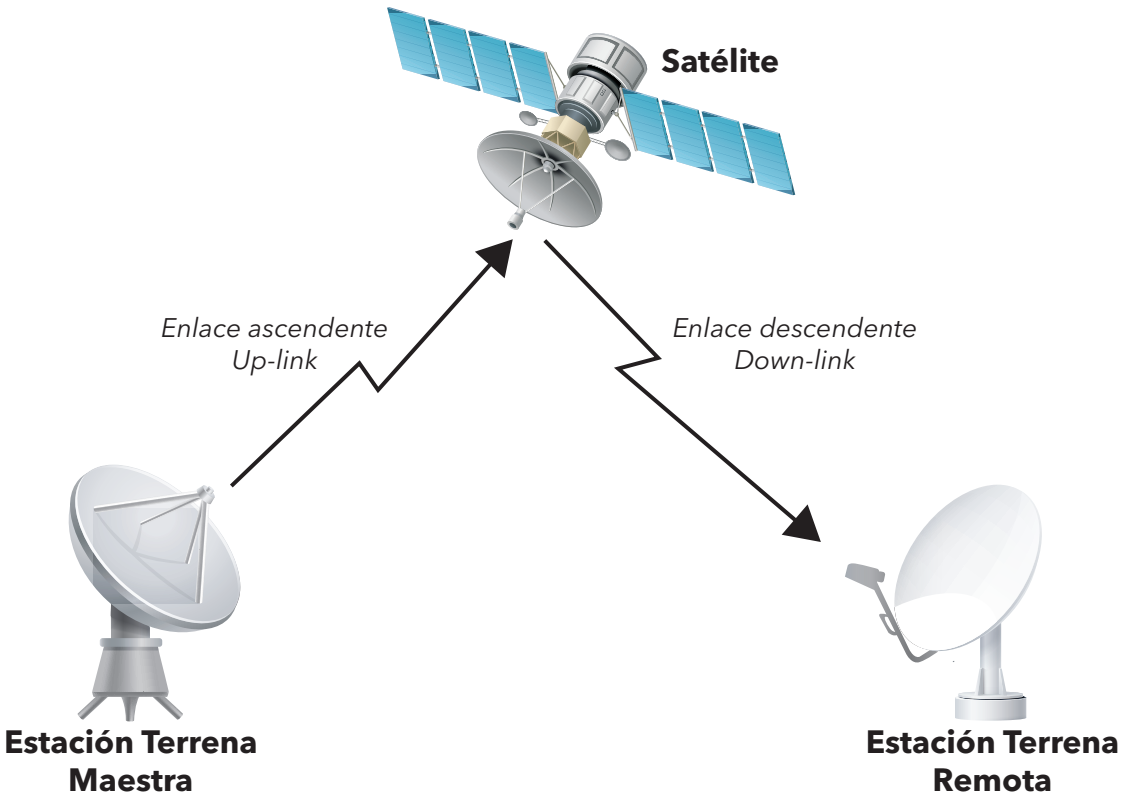


Fuente: Policía Nacional

Figura 6. Parámetros del funcionamiento de la red de comunicaciones de la Policía Nacional

Fuente: Policía Nacional

Figura 7. Red Satelital



Fuente: Policía Nacional

En razón a las condiciones topográficas del territorio colombiano, fue necesario implementar equipos de conexión satelital para garantizar el servicio de voz, datos y video a unidades con difícil conexión, las cuales, a través de estas tecnologías, pueden acceder a los diferentes servicios y aplicaciones desplegadas para el cumplimiento de las actividades operativas, administrativas y docentes.


TOUGHBOOK

RIESGOS, AMENAZAS Y DESAFÍOS

CAPÍTULO 2

RIESGOS, AMENAZAS Y DESAFÍOS

2.1 Gestión permanente de los desafíos

Figura 8. Extracto de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio

Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente al eje estratégico de gestión permanente de los riesgos, amenazas y desafíos.

En este capítulo se presenta la relación de riesgos, amenazas y desafíos considerados durante el diseño de la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio, aclarando que es una información de referencia, complementaria, no excluyente de otros aspectos que se pueden o deban incluir de acuerdo con las especificidades geográficas de cada región y sus dominios (terrestre, fluvial, marítimo, aéreo, espacial, ciberespacial, cognitivo), los sistemas tecnológicos e informáticos existentes, los rangos del espectro electromagnético a utilizar, el conocimiento y experiencia adquirida, así como los momentos históricos y resultados de la gestión con los cuales se evoluciona para generar nuevas capacidades.

Ballesteros (2016) en su publicación "En busca de una Estrategia de Seguridad

Nacional" entiende el riesgo como "aquella hipotética acción que podría llegar a dañar alguno de nuestros intereses nacionales, pero de la que no conocemos con certeza sus características y potencialidades" (p. 48); de igual manera establece una relación entre riesgo, peligro y amenaza así:

> Riesgo es la inseguridad generada por un agente hostil, cuya capacidad para causar efectos dañinos no está constatada a ciencia cierta, pero se considera bastante posible. Cuando el riesgo se constata como una realidad objetiva adquiere la condición de peligro, que se conoce en muchos o todos sus aspectos.
>
> Cuando un agente hostil manifiesta de forma explícita o implícita su voluntad de utilizar ese peligro como un instrumento de coacción para lograr un fin, estaremos ante una amenaza". (p. 49)

Adicionalmente, es preciso mencionar que la estrategia planteada en el presente documento contribuye directamente a fortalecer de la Seguridad Nacional y se alinea con la definición referida por Miguel Ballesteros (2016) y expuesta por Juan Sosa Hurtado director del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) en 1994, en la cual se define a la seguridad nacional como una situación que no presenta amenaza a la soberanía ni a la integridad del territorio y sus habitantes; una situación en la que no existe atentado alguno contra el normal ejercicio de la autoridad ni contra el funcionamiento adecuado de las instituciones; y una situación en que tanto las actividades públicas como las privadas, pueden llevarse a cabo sin obstáculos que se opongan al logro de los más altos niveles de paz, libertad, prosperidad cultural, cívica, moral y económica. (p. 59)

En Colombia a partir de la Ley 1523 de 2012 se definen las bases oficiales para el marco de terminología para la Gestión del Riesgo de Desastres (GRD) por lo cual la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD) fue designada en la coordinación del Sistema Nacional de Gestión del Riesgo de Desastres (SNGRD), recomendando también, a los actores comprometidos de los niveles nacional, departamental y municipal, la incorporación en sus funciones de la terminología incluida en el documento denominado"Terminología sobre la gestión de riesgo de desastres y fenómenos amenazantes 2017" (2017), en el fortalecimiento del trabajo articulado de los entes comprometidos en el territorio nacional.

En la revisión de acciones concretas que permitan neutralizar o mitigar los impactos y efectos no deseados que puedan generarse con motivo de la afectación

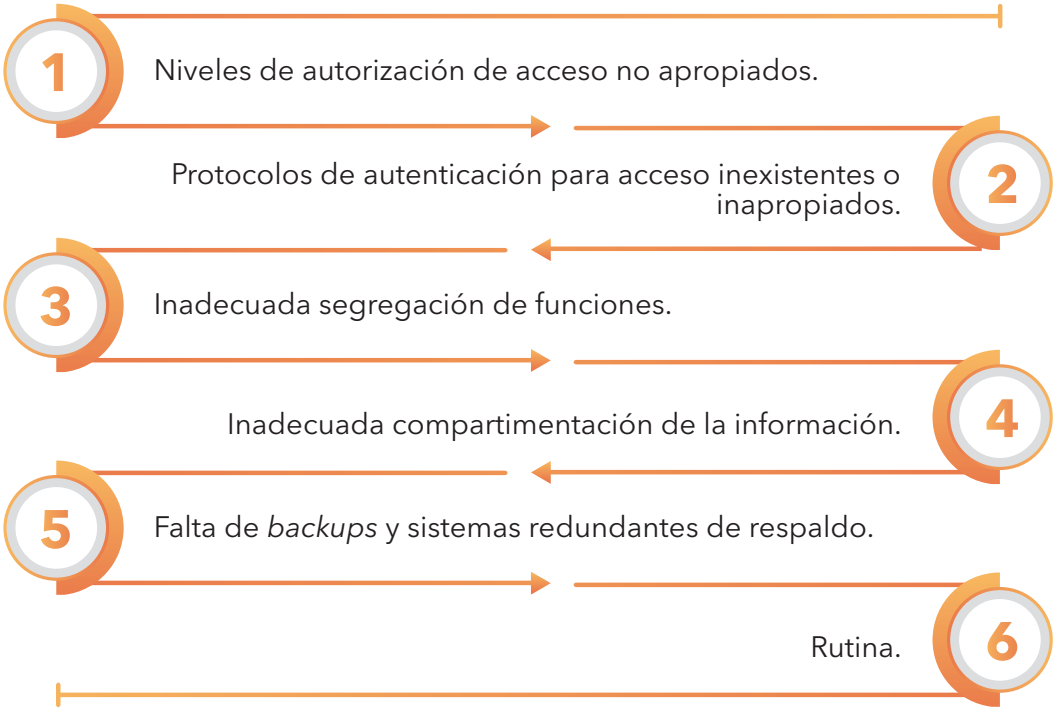
a las redes de comunicación nacional y de conectividad con el ciberespacio utilizadas para la transmisión de voz y datos, es necesario identificar claramente y gestionar los riesgos, amenazas y desafíos que sirven como fundamento en la formulación de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio.

Es necesario identificar claramente y gestionar las amenazas, riesgos y desafíos que sirven como fundamento en la formulación de esta estrategia.

2.2 Riesgos

"Acción hipotética que podría llegar a dañar alguno de los intereses nacionales, pero de la que no se conocen con certeza sus características y potencialidades" (Ballesteros, 2016, p.48)

Figura 9. Riesgos definidos para la estrategia




7
Fuga de información.
8
Falta de control sobre los datos de entrada y salida.
9
Corrupción.
10
Uso de software no autorizados.
11
Falta de normatividad legal vigente o incumplimiento de esta.
12
Personal desmotivado.
13
Altos costos de los servicios provistos por terceros, software, equipos y sistemas asociados.
14
No disponibilidad de capacidades para la transmisión y recepción de voz y datos o conectividad con el ciberespacio por materialización de las amenazas.
15
Los servidores y *hubs* existentes para almacenamiento y distribución de datos.
16
Espacios vacíos del territorio.

17 No contar con *data links* de comunicación propios.

18 La no diferenciación entre comunicaciones operativas y administrativas con la respectiva priorización y niveles de seguridad apropiados.

19 Ausencia de políticas al interior de las entidades e instituciones tanto públicas como privadas relacionadas con el manejo de información con niveles apropiados de clasificación.

20 Información concentrada, sin *backups* o copias de respaldo.

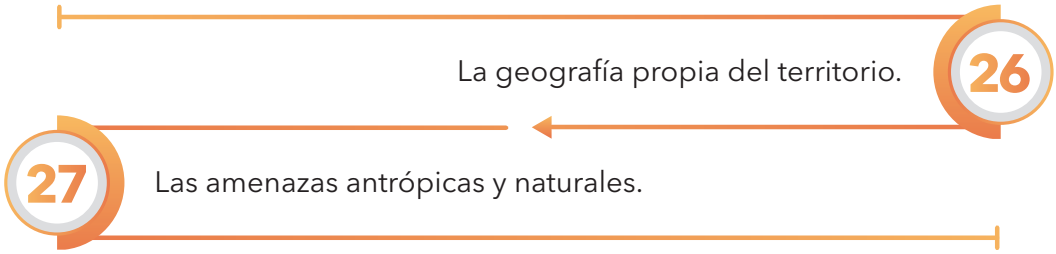
21 Ausencia de lineamientos, políticas, planes o proyectos para el mantenimiento, actualización, renovación de sistemas y equipos, tanto de *hardware* como de *software*.

22 No identificar claramente qué se requiere.

23 Compra de equipos de comunicaciones y sistemas no compatibles entre FF.MM., PNC u otras entidades del Estado.

24 No contar con capacidades satelitales de comunicaciones y observación de la tierra propias.

25 Los fenómenos naturales que afectan la transmisión de voz y datos.

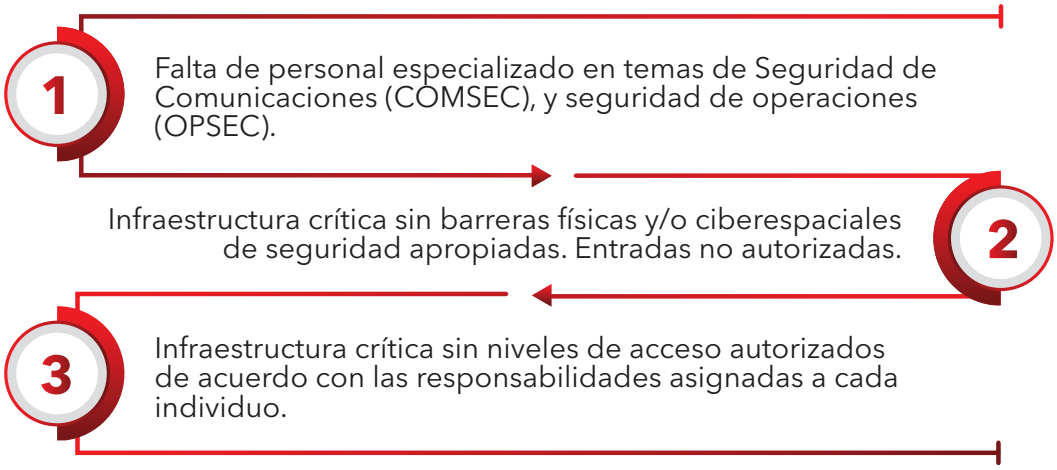


Fuente: Elaboración propia con base en información proporcionada por el grupo de expertos reunido en desarrollo de la materia Estrategia Militar Nacional Aplicada en el curso CAEM-CIDENAL (2022).

2.3 Amenazas

Conforme con lo establecido dentro de la Ley 1523 de 2012 este término hace referencia a un peligro latente, que se relaciona con un evento físico con origen natural que puede ser inducido también por el ser humano a través de sus acciones de forma accidental y que cuando se presenta, se caracteriza porque su severidad puede originar la pérdida de vidas, lesiones u otros impactos en la salud, así como, daños y pérdidas en los bienes, la infraestructura, los medios de producción, los servicios prestados y los recursos del medio ambiente. (Ley 1523 de 2012)

Figura 10. Relación de amenazas para la estrategia




4
Dispositivos de comunicación y terminales relativas al ciberespacio con los niveles de encriptación inapropiados.
5
Inapropiado manejo de las claves de encriptación de equipos de comunicación y de acceso a las salas de reunión o comunicación en el ciberespacio.
6
Otros actores estatales considerados competidores o malignos.
7
Espionaje.
8
Terrorismo.
9
Crimen organizado.
10
Delincuencia común.
11
Ataques cibernéticos.
12
No contar con medios redundantes y alternos.
13
Dependencia estatal de terceros para la gestión de las redes de comunicación, conectividad con el ciberespacio y administración y almacenamiento de la información


14
Contratistas y proveedores del servicio de instalación, mantenimiento y conectividad infiltrados por actores al margen de la Ley o malignos y con problemas legales.
15
Acceso no autorizado a las redes y sistemas de tecnologías de información.
16
Uso no autorizado de dispositivos.
17
Robo y/o pérdida de dispositivos y soportes de almacenamiento.
18
Divulgación de información sensible.
19
Emisiones comprometidas.
20
Comportamientos antiéticos.
21
Interferencias.
22
Interrupción de las redes de comunicación.
23
Interrupción del suministro eléctrico.


24
Coerción, extorsión, corrupción.
25
Suplantación y robos de identidad.
26
Software malicioso.
27
Ingeniería social.
28
Equipos e infraestructura crítica obsoleta y desactualizada.
29
Desconocimiento de las amenazas o inapropiada gestión de estas.
30
Políticas y lineamientos estatales no acordes a las realidades y necesidades tecnológicas. del país
31
Falta de programas estatales que orienten y motiven el desarrollo del conocimiento tecnológico relacionado con redes de comunicación y tecnologías de la información.
32
Falta de normatividad legal vigente para articular las entidades del Estado e instituciones privadas en temas relacionados con las redes de comunicación, conectividad con el ciberespacio y tecnologías de información en general.


33
Planes de desarrollo nacional, departamental y municipales desarticulados y que no contemplan el fortalecimiento de la cobertura de redes de comunicación y de conectividad al ciberespacio del 100 % del territorio nacional.
34
Falta de políticas y lineamientos que propendan por el desarrollo de capacidades de comunicación autónomas.
35
Falta de políticas y lineamientos que contribuyan a la investigación, desarrollo e innovación I+D+I en el campo de las tecnologías de la información y las comunicaciones.
36
Falta de lineamientos estratégicos a nivel estatal que motiven la articulación y sincronización de las entidades del Estado para que se alcance una cobertura del 100 % del territorio en temas de comunicaciones y conectividad con el ciberespacio.
37
Planes de gobierno municipales, departamentales y nacionales que no dan continuidad a los proyectos iniciados previamente o que no incluyen acciones que contribuyan al fortalecimiento, cobertura, comunicaciones y conectividad.
38
Falta de lineamientos y políticas que promuevan la libre competencia en la oferta de servicios, desestimulen el monopolio, pero aseguren de ser necesario la autonomía de funcionamiento del estado y nación.
39
Contratación de terceros sin requerimientos específicos en el objeto contractual, o sin acuerdo de confiabilidad de las señales, calidad de voz y datos recibidos.

40 Falta de acuerdos y alianzas en el escenario internacional que contribuyan al aseguramiento de las comunicaciones y conectividad con el ciberespacio, especialmente en zonas de frontera y ultra territoriales o extracontinentales.

41 Falta de legislación punitiva contra delitos cibernéticos tipo *Phishing, Ransomware,* etc.

42 No contar con mapas municipales (incluyendo zonas veredales), Departamentales y nacionales que permitan identificar capacidades y limitaciones para comunicaciones y conectividad con el ciberespacio del 100 % del territorio (telefonía móvil, telefonía física, comunicaciones microondas, fibra óptica, comunicaciones VHF, UHF, satelital, televisión, radio, emisoras locales).

43 Falta de normatividad legal y acuerdos entre entidades del Estado y la empresa privada que permitan en situaciones de crisis o por seguridad nacional, el que emisoras de radio y canales de televisión nacionales o que operan en el país puedan articularse a nivel local para transmitir información de manera masiva (tipo broadcast) y focalizada hacia un sector de interés por parte de autoridades locales responsables de gestionar las situaciones presentadas en un momento determinado.

44 No contar con sistemas de alertas tempranas que permitan identificar zonas donde se presentarán situaciones críticas para anticipar el manejo requerido de comunicaciones y de conectividad con el ciberespacio para que las autoridades, entidades o personal designado pueda desarrollar las acciones necesarias de gestión de la situación.

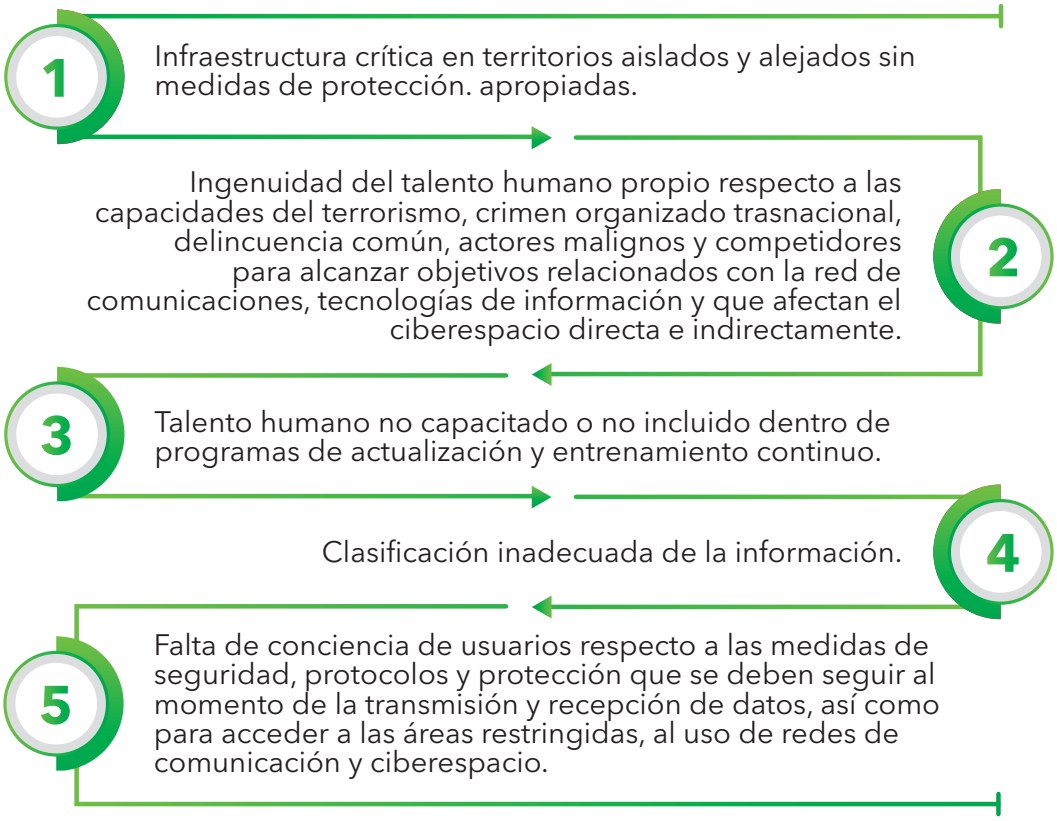

45
Violación de Leyes y la normatividad vigente.
Falta de lineamientos para la renovación tecnológica y adquisición de equipos estandarizados que cuenten con una evaluación previa de seguridad por parte de las autoridades competentes del orden nacional.
46
47
No contar con lineamientos y políticas que orienten a los gobiernos municipales, departamentales y nacionales para destinar recursos y gestionar acuerdos que aseguren la comunicación y conectividad del 100 % del territorio.
No se cuenta con políticas de sanitización de equipos al interior de las entidades e instituciones del Estado.
48
49
Niveles de acceso no validados y/o autorizados.
Planes de capacitación, entrenamiento y reentrenamiento en temas de seguridad y ciberseguridad no establecidos de manera periódica.
50
51
Ausencia de políticas mandatorias de *backups* periódicos.
Desastres naturales.
52

Fuente: Elaboración propia con base en información proporcionada por el grupo de expertos reunido en desarrollo de la materia Estrategia Militar Nacional Aplicada en el curso CAEM-CIDENAL (2022).

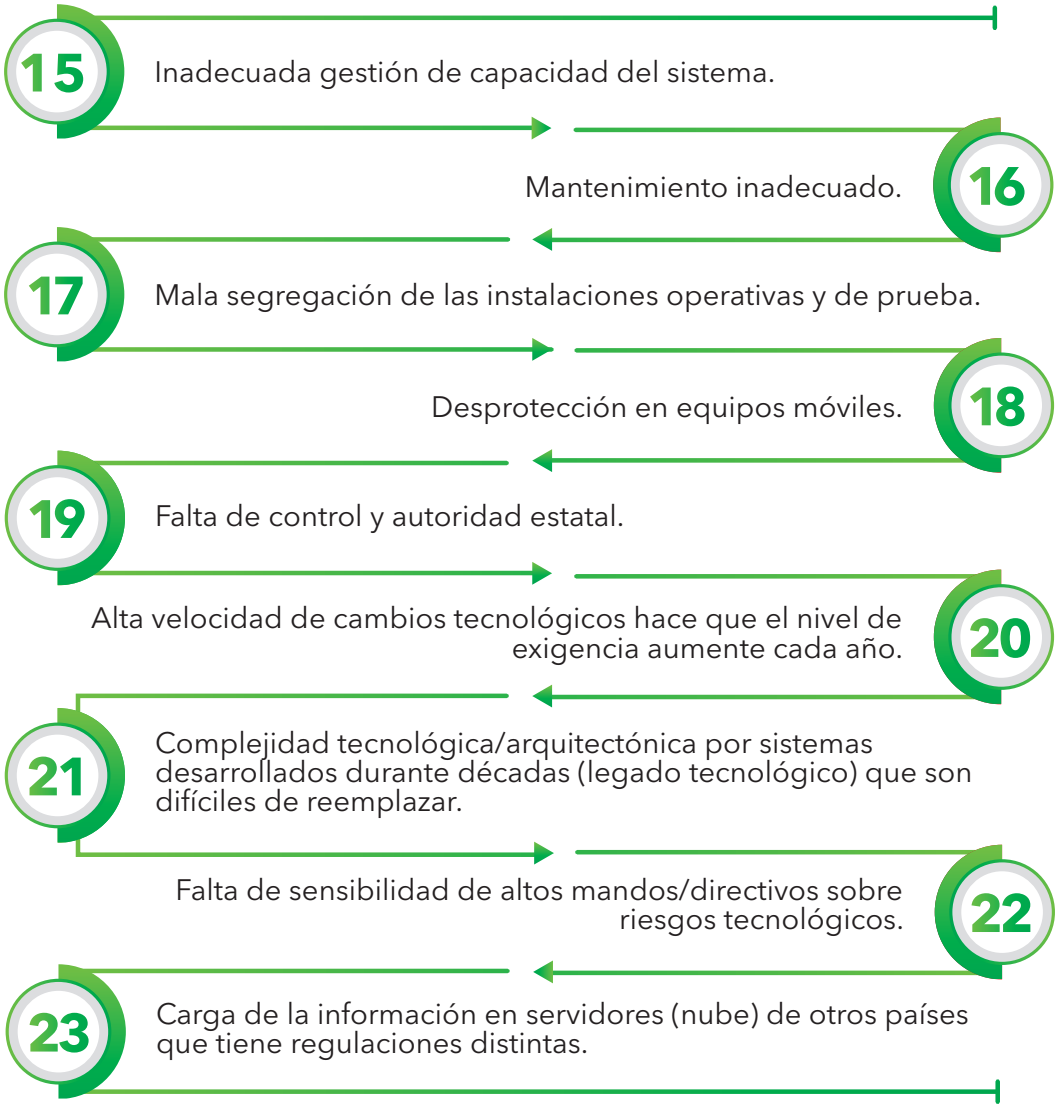
2.4 Desafíos (vulnerabilidades)

El Congreso de la República determina en la Ley 1523 de 2012 que los desafíos se definen como una susceptibilidad o fragilidad física, que se presenta en la economía, el entorno social, ambiental e institucional y en una comunidad que puede ser objeto de efectos adversos derivados de un evento físico. Es natural a la predisposición de los seres humanos a sufrir pérdidas o daños en sus medios de subsistencia, sus sistemas físicos, sociales, económicos y de apoyo, los cuales pueden ser afectados por eventos físicos peligrosos (Ley 1523 de 2012).

Figura 11. Relación de desafíos para la estrategia




6
Falta de conciencia.
7
Sistemas tecnológicos complejos.
8
Claves de acceso a instalaciones y equipos poco complejas.
9
La distribución actual de repetidores y equipos utilizados para la transmisión y recepción. de voz y datos.
10
Los sistemas de generación de energía que alimentan los equipos (red comercial, generadores, paneles solares, banco de baterías, etc.).
11
El tamaño del territorio y largas distancias a cubrir.
12
No contar con plataformas terrestres, marítimas, fluviales y aéreas que se puedan desplegar rápidamente hacia áreas de interés, para que sirvan como estaciones de comunicaciones y/o repetidores para la gestión de crisis.
13
Sensibilidad del equipo a los cambios de voltaje.
14
Inadecuada seguridad del cableado.


15
Inadecuada gestión de capacidad del sistema.
16
Mantenimiento inadecuado.
17
Mala segregación de las instalaciones operativas y de prueba.
18
Desprotección en equipos móviles.
19
Falta de control y autoridad estatal.
20
Alta velocidad de cambios tecnológicos hace que el nivel de exigencia aumente cada año.
21
Complejidad tecnológica/arquitectónica por sistemas desarrollados durante décadas (legado tecnológico) que son difíciles de reemplazar.
22
Falta de sensibilidad de altos mandos/directivos sobre riesgos tecnológicos.
23
Carga de la información en servidores (nube) de otros países que tiene regulaciones distintas.

24 Legislación que genera limitantes al despliegue tecnológico. Un ejemplo: Legislación en la que prima la gestión de intereses nacionales vs acceso a la mejor tecnología (ej. servicios en la nube/traslado de datos al exterior limitados si hay dependencias de países terceros).

25 Legislación inadecuada (anticuada) para perseguir crímenes tecnológicos modernos.

26 Limitaciones geopolíticas que impidan acceder a la mejor tecnología (China, oriente vs Occidente).

27 Falta de limitaciones de interoperabilidad entre proveedores tecnológicos.

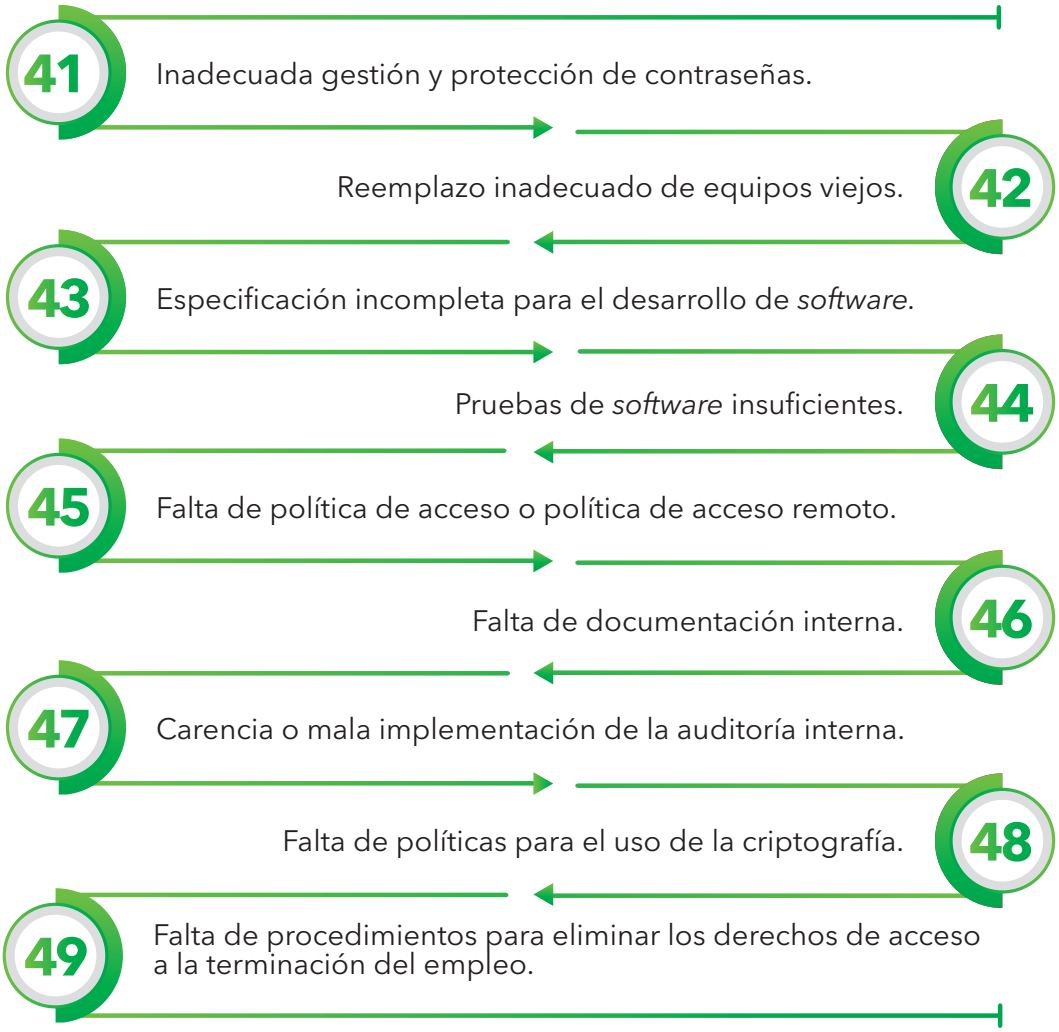
28 Debilidades de ecosistema. Es decir, interconexiones con dependencias de terceros para ciertos servicios. Una tipología son las debilidades de proveedores (ej. ataques a terceros que imposibilita provisión de servicio).

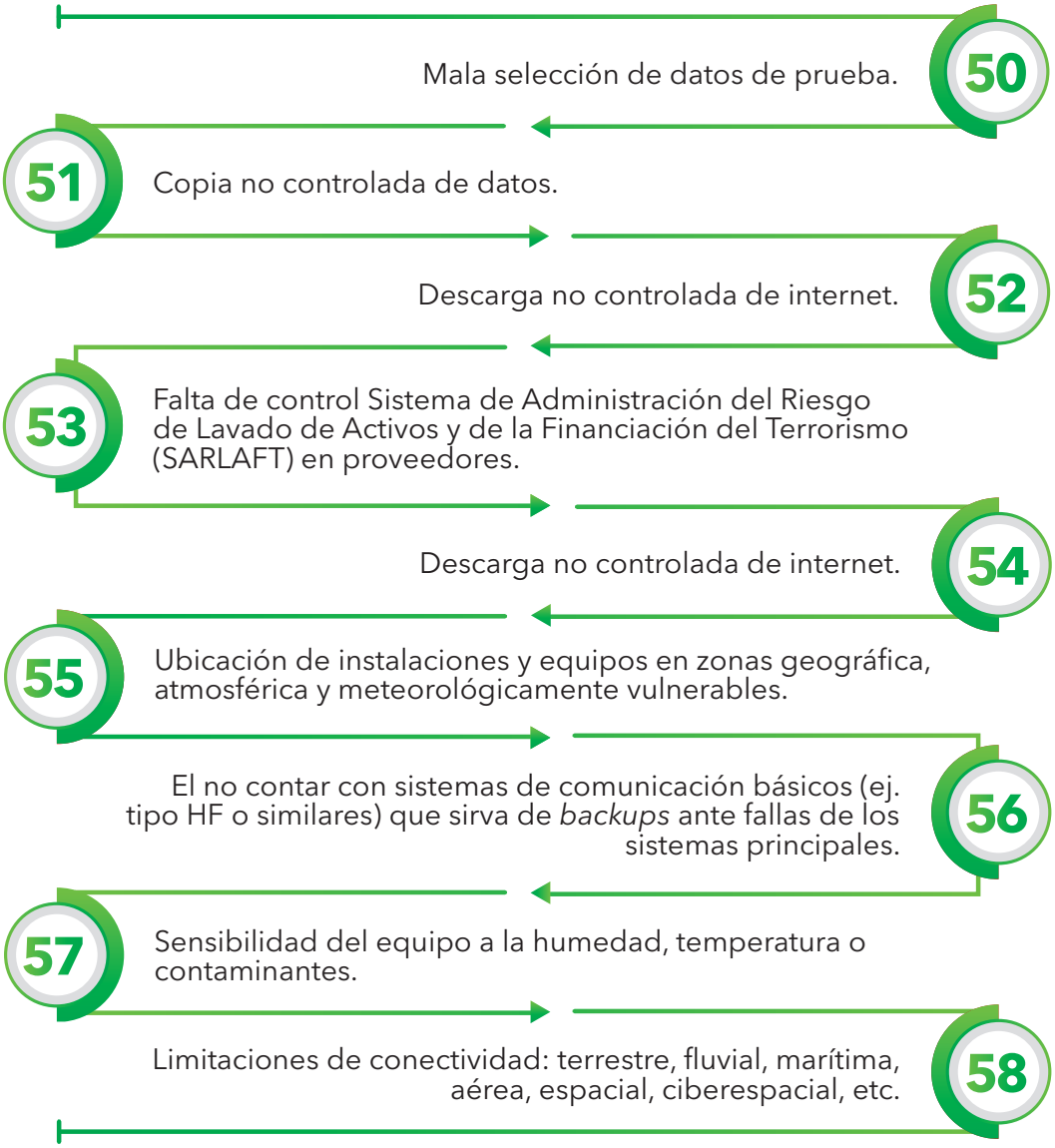
29 Herramientas tecnológicas obsoletas.

30 Alta rotación de empleados en áreas de seguridad virtual/ tecnológica.

31 Sistemas de recuperación de servicio inadecuados.


Ausencia de políticas y normatividad que motive la libre competencia.
32
33
Recursos insuficientes para inversiones relacionadas.
Falta o insuficiencia de herramientas y equipos.
34
35
Falta de personal capacitado (ej. CSIRT D. 338/22 o Coordinación Nacional de Seguridad Digital D. 338/22).
Falta de formación y conocimiento por parte de los empleados.
36
37
Pólizas de seguros incompletas para cubrir los riesgos.
Gestión inadecuada del cambio.
38
39
Inadecuada gestión de red.
Respaldo inapropiado o irregular.
40


41
Inadecuada gestión y protección de contraseñas.
42
Reemplazo inadecuado de equipos viejos.
43
Especificación incompleta para el desarrollo de *software*.
44
Pruebas de *software* insuficientes.
45
Falta de política de acceso o política de acceso remoto.
46
Falta de documentación interna.
47
Carencia o mala implementación de la auditoría interna.
48
Falta de políticas para el uso de la criptografía.
49
Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.



Fuente: Elaboración propia con base en información proporcionada por el grupo de expertos reunido en desarrollo de la materia Estrategia Militar Nacional Aplicada en el curso CAEM-CIDENAL (2022).

SINCRONIZACIÓN Y ARTICULACIÓN DEL ESTADO - EJES ESTRATÉGICOS

CAPÍTULO 3

Figura 12. Articulación del Estado - Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio

Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente en la articulación del Estado y ejes estratégicos.

3.1 Sincronización y articulación en el nivel estratégico del Estado

Figura 13. Bloque central Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio

Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente al bloque central.

Las proyecciones para el fortalecimiento de las redes de comunicación nacionales que permitan la transmisión de voz y datos en ambientes multidominio y a través del ciberespacio, deben ser consideradas como acciones a ejecutar en beneficio del Estado, cuya responsabilidad directa inicial recae en los gobiernos de turno que velan y propenden por un país moderno, actualizado tecnológicamente, con capacidad de transmitir y recibir voz y datos por canales multiespectrales, redundantes en los que se incluye el ciberespacio.

Estas facilidades que se presentan en las dinámicas vigentes contribuyen al crecimiento económico y desarrollo de un país con complejidades geográficas e irregularidades que afectan a la población en el territorio, quienes requieren estar conectados y comunicados para mantener e incrementar la seguridad lo cual impacta en el bienestar de la población y la cobertura de las necesidades básicas para conseguir una calidad de vida digna.

El Gobierno nacional a través de la visión responsable de gobernanza sobre el territorio e integración de las comunidades más alejadas, debe seguir fortaleciendo las capacidades del país en torno a las tecnologías de la información y comunicaciones en los planes de desarrollo. La expansión de programas como "Colombia vive digital" e iniciativas para la generación de energía por fuentes alternativas para núcleos sociales y familiares aislados en el territorio, son un claro ejemplo de los esfuerzos que deben

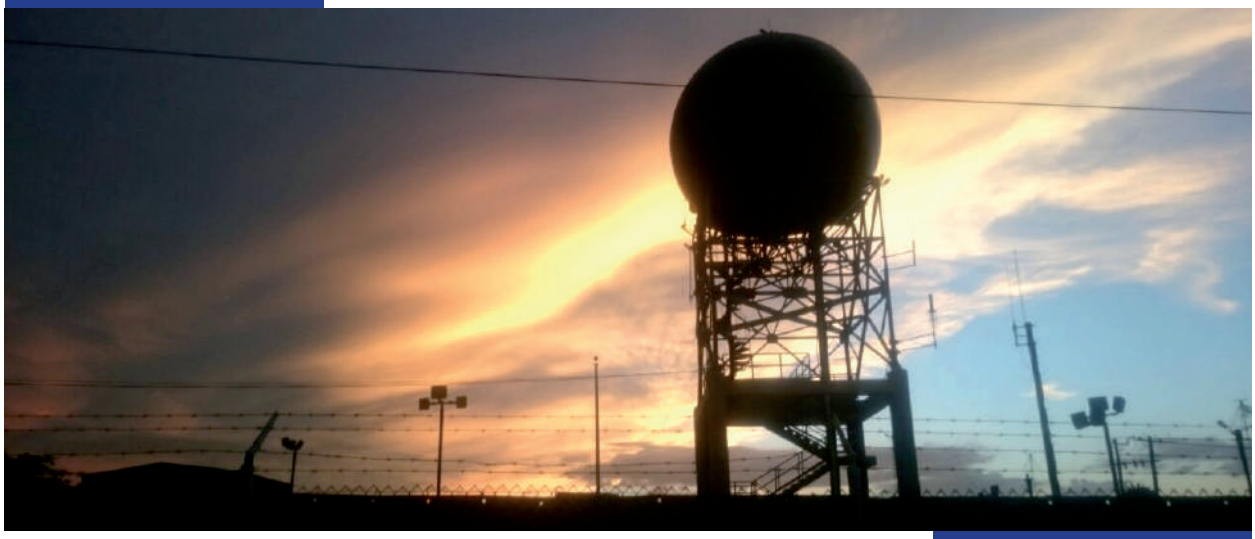
consolidarse en la provisión de la energía necesaria para el uso de terminales con las que estas comunidades puedan tener acceso al ciberespacio.

El Ministerio de Tecnologías de la Información y las Comunicaciones o el ente de gobierno de mayor preponderancia en su momento, como principal entidad articuladora y visionaria en términos de tecnología, comunicaciones y conectividad, debe continuar incrementando las capacidades de comunicación y cobertura al 100 % del territorio nacional, con alcance global y en el espacio exterior, facilitando comunicaciones multidominio a partir de la planeación, revisiones periódicas y ajustes a los planes estratégicos, correspondientes de acuerdo a la evolución tecnológica y necesidades del momento.

Las diferentes entidades del Estado, ministerios e instituciones del orden nacional, departamental y municipal en general requieren de la articulación guiada por los objetivos del alto gobierno y los planes estratégicos del Ministerio de Tecnologías de la Información y las Comunicaciones, incluyendo dentro de sus planes locales de desarrollo acciones tendientes a fortalecer la comunicación y conectividad del 100% de su territorio, demandando la ejecución de diagnósticos alineados desde el nivel central para identificar el nivel de la cobertura actual, las capacidades existentes, el tipo de tecnología, las prioridades relacionadas con tecnologías a implementar de acuerdo a las condiciones del terreno, características ambientales u otras que lo puedan afectar y un faseamiento de avance periódico, sujeto a planes estratégicos que no dependan exclusivamente de voluntades pasajeras de gobernantes de turno sino que articulen la intención estratégica del Estado como un todo.

En concordancia con lo anterior, es fundamental que exista la articulación del Estado, representado por el Gobierno nacional, departamental y municipal con la empresa privada, otro tipo de instituciones y la comunidad en general, ya que la creación de oportunidades de libre mercado y competencia ajustadas a las necesidades de la población favorecen la contribución a los procesos de estabilización y consolidación del territorio, mediante la articulación, sincronización del conocimiento y capacidades existentes, para generar acciones sinérgicas que permitan gestionar de la mejor manera los desafíos vigentes y los que se presenten en el corto, mediano y largo plazo.

Bajo esa perspectiva, como actores fundamentales a considerar para el planeamiento e implementación de la estrategia de seguridad de redes de comunicación y conectividad con el espacio y ciberespacio se establece a las Fuerzas Militares y Policía Nacional de Colombia, las cuales ejecutan un esfuerzo



Revista Aeronaútica Fuerza Aérea Colombiana

enfocado en la seguridad y defensa de la nación frente a amenazas externas, pero también; de las que se producen a nivel interno en el país.

El conocimiento de las amenazas potenciales que puedan ser consideradas antrópicas o generadas por las personas que están al margen de la ley se pronostican para ciertas regiones del país, considerando también, eventos críticos o naturales que se puedan presentar. Las Fuerzas Militares y la Policía Nacional junto con otras entidades e instituciones del orden nacional e internacional son los primeros llamados para actuar en la protección de vidas, evitar el dolor y sufrimiento humano, evitar las pérdidas materiales y devolver las condiciones normales de vida rápidamente, para lo cual; las comunicaciones y capacidad de transmisión de voz, datos, imágenes fotográficas o video en tiempo real son fundamentales.

Las Fuerzas Militares y Policía Nacional necesitan fortalecer su capacidad de interoperabilidad con medios de comunicaciones compatibles, estandarizados y redundantes, con seguridad de voz, modernos y actualizados, incluyendo canales de conectividad a través del ciberespacio capaces de sincronizarse con otros organismos investigativos, de seguridad, vigilancia e inteligencia del orden nacional como internacional.

El talento humano como factor fundamental de la estrategia a desarrollar en temas de conectividad, también debe continuar potenciando su conocimiento en áreas relacionadas aprovechando todos los entornos académicos, además de aquellos orientados a la actualización de los empleados de las empresas e instituciones estatales y privadas que suministren educación pública de fácil acceso.

Los componentes físicos que facilitan la conectividad a través del ciberespacio como activos estratégicos de la nación, demandan de las autoridades civiles, militares y policiales a lo largo del territorio nacional, precisión en la definición de las riesgos, amenazas y desafíos en su área de responsabilidad, así como la gestión reflejada en las estrategias necesarias para mitigarlos, generando acciones preventivas y proyectando presupuestos complementarios tanto para empresas privadas de seguridad como para las Fuerzas Militares y Policía Nacional, en la consolidación de la capacidad diferencial para cada una de estas.

De manera general, la estrategia de seguridad de redes de comunicación y conectividad con el ciberespacio define dos objetivos estratégicos, establece cinco líneas de esfuerzo y un

Revista Aeronaútica Fuerza Aérea Colombiana

eje estratégico que agrupa acciones relacionadas en tres tareas específicas, cada una con 6, 5 y 8 factores de análisis.

Es oportuno mencionar que la estrategia debe ser considerada como complementaria y no excluyente para aspectos previamente implementados por las diferentes entidades del Estado y que sirven como insumo para construir desde el nivel municipal, departamental o nacional, capacidades que aporten a la articulación de los líderes civiles y militares en el logro de objetivos comunes, razón por la cual propone como responsables a quienes intervienen en el proceso y que se encargan también de promover la integridad del territorio, mediante el mantenimiento de una sociedad unida, informada y comunicada, en los lugares más más alejados de la seguridad, en donde conviven usuarios que se benefician directa e indirectamente de estas capacidades en tiempo de paz o en tiempos de crisis.

3.2 Ejes estratégicos

3.2.1 Diagnóstico actual y proyección del estado final deseado

El proceso de evolución de los Estados siempre ha requerido implementar, mantener, mejorar, actualizar y renovar periódicamente las tecnologías de información, comunicaciones y conectividad con el ciberespacio, facilitando los procesos de interrelación de sus gobiernos, ciudadanos y población en general, para mejorar la gestión efectuada mediante las actividades públicas y privadas que contribuyen al crecimiento económico, seguridad, desarrollo y bienestar.

En concordancia con lo previamente expuesto, es actividad prioritaria por parte de quienes asumen la responsabilidad de continuar gestionando las acciones para ampliar las coberturas de comunicaciones y conectividad con el ciberespacio en la totalidad de su territorio, revisar y conocer el estado actual de los sistemas tecnológicos principales y de apoyo que contribuyen a la gobernanza, seguridad y desarrollo en su región, buscando identificar el tipo de tecnologías existentes en el área de responsabilidad asignada, así como las necesidades de seguridad y protección a implementar en las instalaciones y componentes relacionados, tanto principales como alternos que son considerados como críticos, la cobertura real de comunicaciones multiespectrales y en los multidominios, los proyectos anteriores en desarrollo y las necesidades generales de los diversos actores que dinamizan la nación para construir un plan de acción que complemente, priorice, focalice y maximice el uso de los recursos asignados.

3.2.2 Cobertura y redundancia de comunicaciones multidominio

Figura 14. Cobertura y redundancia multidominio

Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente al eje estratégico de cobertura y redundancia de comunicaciones multidominio.

El Estado, su gobierno, liderazgo civil, militar, policial, autoridades y en general los actores interesados en que se tenga una cobertura plena de comunicaciones sobre el territorio, debe considerar como medida de mitigación de riesgo y rápida respuesta para restaurar el servicio afectado en un momento determinado, el contar con equipos, redes de comunicación y para la conectividad redundantes o alternos en un área o región determinada, que permitan canalizar rápidamente la voz y datos requeridos para transmitir o recibir.

- **Municipal (urbano y veredal), departamental y nacional**

Corresponde al liderazgo civil del orden municipal, departamental y nacional, conocer las capacidades y limitaciones que tiene las comunicaciones y conectividad con el ciberespacio en sus territorios, regiones y áreas de responsabilidad asignada; para lo cual las autoridades pertinentes deberán consolidar periódicamente, por medio de las respectivas oficinas de planeación o sus equivalentes, el inventario de infraestructura relacionada con el asunto que se puede considerar crítica en su área de responsabilidad asignada.

De igual forma, los mandatarios locales a nivel municipal deben adelantar las gestiones correspondientes con autoridades civiles, militares, policiales y la empresa privada, según corresponda, para determinar y graficar la cobertura real de comunicaciones y estado de la conectividad con el ciberespacio en su territorio incluyendo las zonas veredales.

Ante la variedad de medios de comunicación que utilizan el espectro electromagnético, la oferta de proveedores

que suministran a nivel local, regional y nacional los servicios de telefonía y de conectividad con el ciberespacio; se propone que como mínimo el liderazgo civil que actúa a nivel regional, tenga un pleno conocimiento de las coberturas de comunicaciones y el tipo de equipos que se emplean en jurisdicción, para identificar riesgos, amenazas y desafíos, determinar necesidades, identificar oportunidades y encauzar los planes de acción, que permitan neutralizar o mitigar los posibles impactos derivados de la ausencia de comunicaciones positivas con las personas (naturales y jurídicas) ubicadas en su territorio.

LÍDER CIVIL

Debe conocer y verificar las características de la cobertura de comunicaciones y conectividad en su territorio, con el fin de facilitar el proceso de toma de decisiones en tiempos normales o de crisis, identificando como mínimo lo siguiente:

1. Cantidad de abonados telefónicos fijos y nombre de las empresas prestadoras del servicio en su municipio (incluyendo zonas veredales).
2. Mapas de cobertura de telefonía fija a nivel municipal por cada uno de los proveedores de servicio existentes y estadísticas de crecimiento, estabilidad o decrecimiento.
3. Graficación sobre el mapa municipal, de las coberturas de servicio prestado por diferentes operadores de telefonía fija.

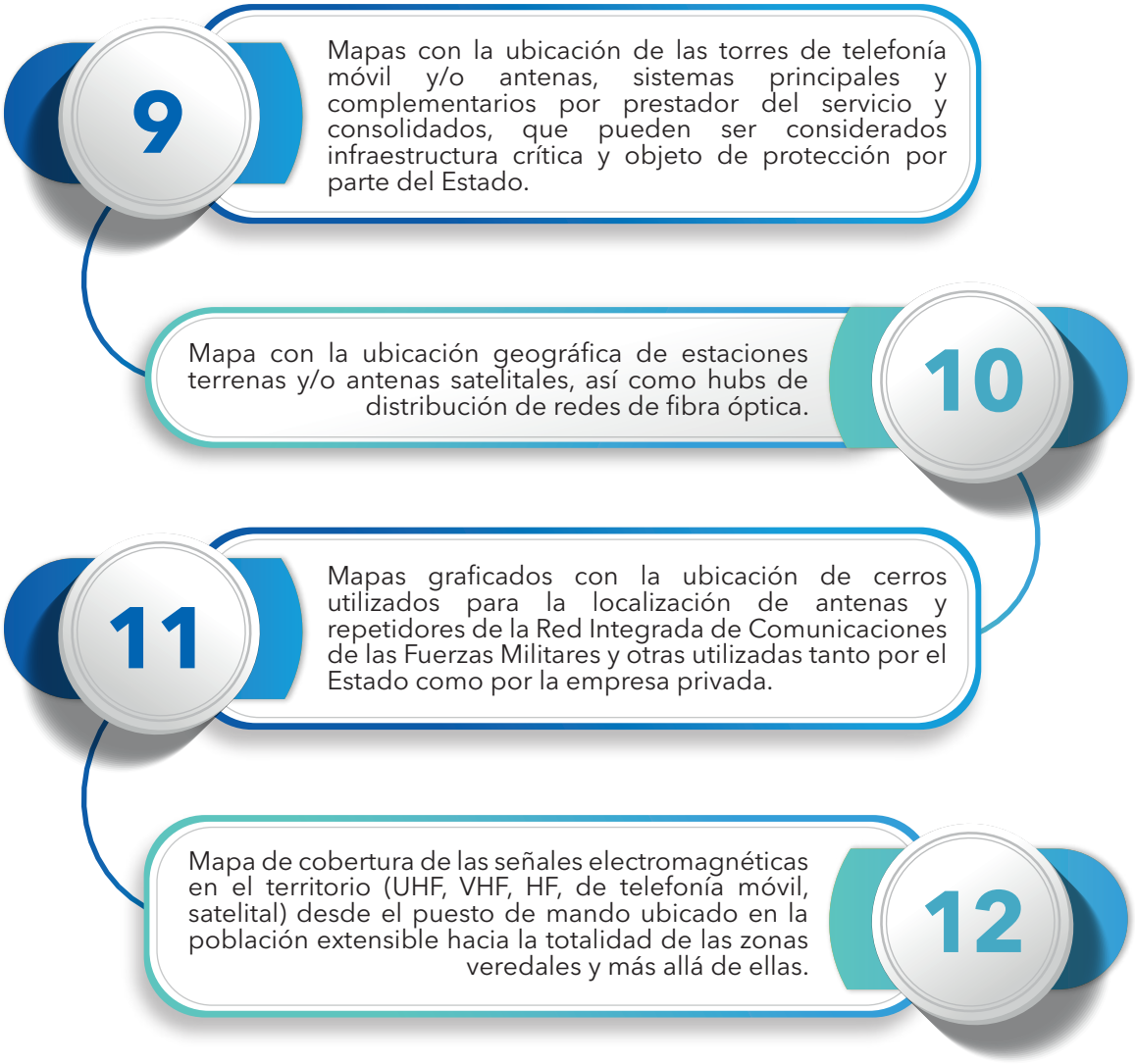
4. Costos y tarifas promedio de los servicios prestados de telefonía fija, de acuerdo con la clasificación de comercial o residencial, zonificación y estrato correspondiente.

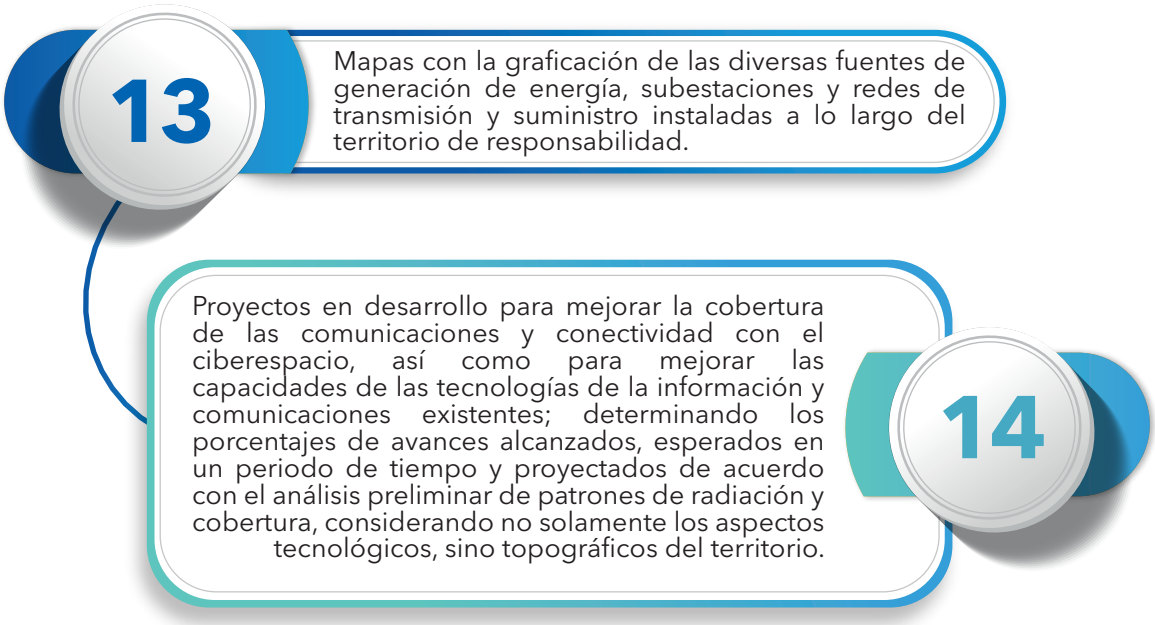
5. Cantidad de usuarios de telefonía móvil y nombre de las empresas prestadoras del servicio en su municipio (incluyendo zonas veredales).

6. Mapas de cobertura de telefonía móvil por cada uno de los proveedores de servicio existentes y estadísticas de crecimiento, estabilidad o decrecimiento, así como comparativas a nivel municipal.

7. Mapas con la ubicación y cobertura de centros de acceso digital para conexión con el ciberespacio en las veredas.

8. Mapas con los resultados de análisis gráficos de cobertura de comunicaciones y conectividad con el ciberespacio, que permitan visualizar las zonas del territorio consideradas, cubiertas plenamente con sistemas redundantes, alternos y con calidad de señal confiable (verde), que se encuentran en implementación prioritaria y cuentan con al menos un sistema de comunicación principal y uno alterno, con calidad de señal poco confiable y/o limitada (amarillo) y que se encuentran sin cobertura permanente de al menos un sistema de comunicación, es inexistente o no hay una señal confiable (rojo).


9
Mapas con la ubicación de las torres de telefonía móvil y/o antenas, sistemas principales y complementarios por prestador del servicio y consolidados, que pueden ser considerados infraestructura crítica y objeto de protección por parte del Estado.
Mapa con la ubicación geográfica de estaciones terrenas y/o antenas satelitales, así como hubs de distribución de redes de fibra óptica.
10
11
Mapas graficados con la ubicación de cerros utilizados para la localización de antenas y repetidores de la Red Integrada de Comunicaciones de las Fuerzas Militares y otras utilizadas tanto por el Estado como por la empresa privada.
Mapa de cobertura de las señales electromagnéticas en el territorio (UHF, VHF, HF, de telefonía móvil, satelital) desde el puesto de mando ubicado en la población extensible hacia la totalidad de las zonas veredales y más allá de ellas.
12



- **Antenas y repetidores**

EEs indispensable conocer de manera precisa la ubicación geográfica de antenas y repetidores, así como de las redes de transmisión en el territorio, para analizar periódicamente de manera conjunta, interagencial, coordinada y con la empresa privada, las riesgos, amenazas y desafíos a las que están expuestas estas instalaciones y determinar con el concurso de las autoridades, los niveles de seguridad que se deben implementar para evitar afectaciones en la transmisión y recepción de voz y datos, así como para conectarse con el ciberespacio; articulando y gestionando las capacidades diferenciales que cada actor aporta para incrementar los niveles de seguridad requeridos.

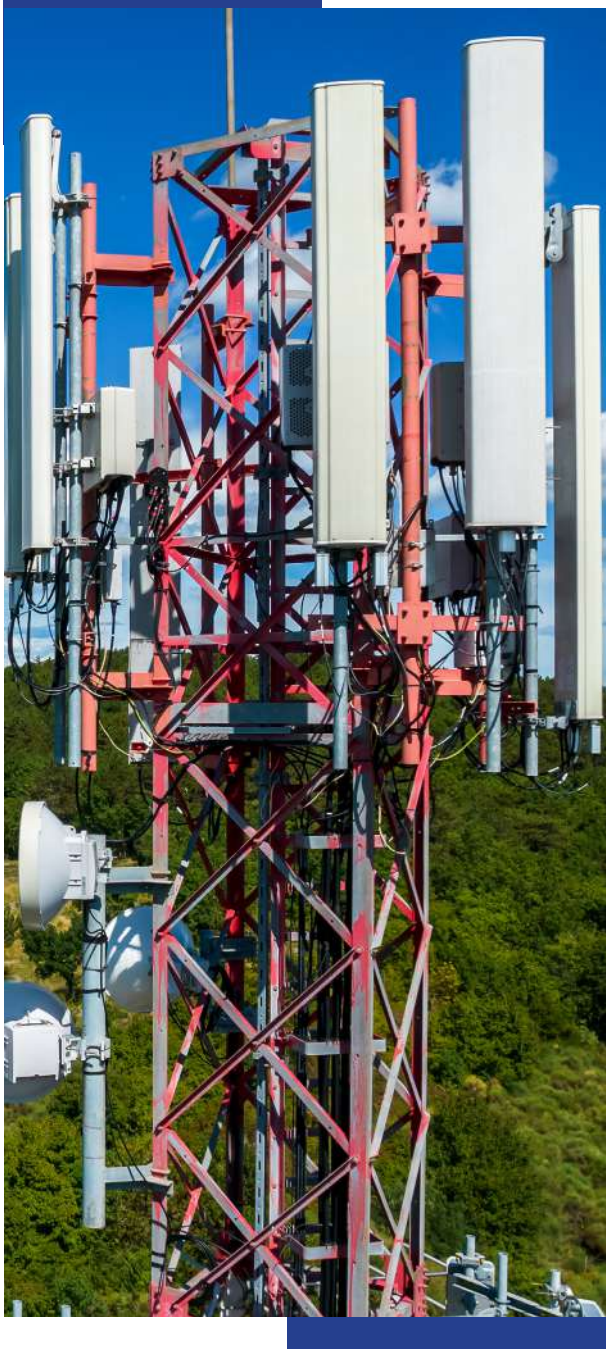
- **Hubs de fibra óptica**

El conocimiento de la ubicación de los hubs y/o terminales de fibra óptica, así como del cableado principal y alterno

de transmisión en el territorio, facilita el análisis periódico de manera conjunta, interagencial, coordinada y con la empresa privada, los riesgos, amenazas y desafíos a los que están expuestas estas instalaciones y determinar con el concurso de las autoridades, los niveles de seguridad que es preciso implementar para evitar afectaciones en la transmisión y recepción de voz y datos, así como para conectarse con el ciberespacio; articulando y gestionando las capacidades diferenciales que cada actor puede aportar para incrementar los niveles de seguridad requeridos.

- **Estaciones terrenas**

Se debe conocer de manera precisa la ubicación de las estaciones terrenas utilizadas para la recepción y transmisión de información satelital, incluyendo también el análisis conjunto, interagencial, coordinado y con la empresa privada, de riesgos, amenazas y desafíos a las que están expuestas estas instalaciones para determinar, con el concurso de las autoridades, los niveles de seguridad que es preciso implementar para prevenir afectaciones en la transmisión, recepción de voz y datos, así como para conectarse con el ciberespacio; articulando y gestionando las capacidades diferenciales que cada actor puede aportar para incrementar los niveles de seguridad requeridos.



- **Data centers**

El conocimiento preciso de la localización de los *Data centers* principales y alternos es indispensable, al igual que los análisis producidos de manera conjunta, interagencial, coordinada y con la empresa privada, las riesgos, amenazas y desafíos a las que están expuestas estas instalaciones y determinar con el concurso de las autoridades, los niveles de seguridad que es preciso implementar para evitar afectaciones en la transmisión y recepción de voz y datos, así como para conectarse con el ciberespacio; articulando y gestionando las capacidades diferenciales que cada actor puede aportar para incrementar los niveles de seguridad requeridos.

- **Otros**

Los elementos mencionados se pueden considerar como los componentes principales de algunos de los sistemas de transmisión, recepción de voz y datos y para la conectividad con el ciberespacio; sin embargo, esta información no limita la inclusión de otros componentes principales y/o alternos utilizados en ciertas regiones con características geográficas específicas, que manejan tecnologías diferenciales en proceso de experimentación o implementación.

3.2.3 Gestión permanente de los desafíos[1]

- **Priorizar la seguridad requerida para la infraestructura crítica**

Teniendo en cuenta el diagnóstico actual y la proyección del estado final deseado, así como riesgos, amenazas y desafíos descritas en el capítulo 3 del presente documento; además del análisis realizado por las autoridades municipales y la determinación de las ARV que pueden afectar las redes de comunicación nacional y la conectividad con el ciberespacio en sus áreas veredales asignadas. Corresponde al liderazgo civil, en coordinación con un grupo de expertos en el que se incluyan las autoridades civiles, militares, policiales y comprometidas en actividades de atención y prevención de emergencias y cuando fuere necesario la empresa privada, elaborar una matriz de análisis y evaluación del riesgo específica para su sector, con la cual se pueda determinar cuál es la infraestructura crítica afín con las tecnologías de información y comunicaciones que se deben proteger de forma prioritaria, asignando adicionalmente un responsable de consolidar, gestionar, articular, conciliar y asignar las responsabilidades de protección y seguridad de puntos críticos.

A partir de ello, se formula un ejemplo base propuesto:

[1] La profundización relacionada con los riesgos, amenazas y desafíos contemplados en la Estrategia de Seguridad para las redes de Comunicación Nacional y Conectividad para el Ciberespacio se encuentran descritas en el capítulo 3 del presente documento.

Tabla 1. Matriz de análisis y priorización de riesgos, amenazas y desafíos para la sincronización y asignación de responsabilidades de seguridad y protección a la infraestructura crítica

Matriz de análisis y priorización de riesgos, amenazas y desafíos para la sincronización y asignación de responsabilidades de seguridad y protección a la infraestructura crítica													
N°	Componente del sistema	Nombre	Coordenadas	NIVEL DE SEGURIDAD Y PROTECCIÓN REQUERIDO			ENTIDAD QUE PROVEERA SEGURIDAD Y PROTECCIÓN					
				Alto	Medio	Bajo	EJC	ARC	FAC	PNC	OTRO	EMPRESA PRIVADA
1	Cerro de comunicaciones 1	Cerro el tigre	2°43'25" N / 69°20'24"W	X					X			
2	Cerro repetidor 1	Cerro el cable	4°43'03" N / 74°05'16" W	X			X					
3	Antena de comunicación celular empresa N-1	Barrio La Libertad	X°XX'XX" N / XX°XX'XX" W			X						X
4	Antena de comunicación celular empresa N-2	Vereda El Espino	X°XX'XX" N / XX°XX'XX" W		X					X		
5	Hubs de fibra óptica nombre N-1	Puerto Esperanza	X°XX'XX" N / XX°XX'XX" W	X				X				
6	Hubs de fibra óptica nombre N-2	Caribe 1	X°XX'XX" N / XX°XX'XX" W		X					X		
7	Data center N-1	CATAM	X°XX'XX" N / XX°XX'XX" W	X					X			
8	Estación terrena N-1	CAN	X°XX'XX" N / XX°XX'XX" W	X			X					
9	Subestación eléctrica	OCOA	X°XX'XX" N / XX°XX'XX" W			X				X		
10	Torre de energía	E-2 Energy	X°XX'XX" N / XX°XX'XX" W		X			X				

Fuente: Elaboración propia. Ejemplo de referencia propuesto

- **Planeamiento conjunto, coordinado e interagencial de la seguridad**

Una vez definidas las prioridades y asignadas las responsabilidades de protección de equipos, instalaciones, redes e infraestructura considerada, crítica u otros; corresponde a cada uno de los líderes militares, policiales y de empresas de seguridad realizar una verificación inicial sobre el terreno que permita validar la información previamente recibida, incorporar nuevos elementos de juicio desde su área de experticia y elaborar un planeamiento específico en el punto de interés y sus alrededores,

fijando claramente el objetivo, medios necesarios y formas para utilizarlos.

Después de desarrollada la actividad previamente descrita, los líderes militares, policiales y de empresas de seguridad se reunirán de manera conjunta, coordinada e interagencial con el liderazgo con el representante municipal o departamental para presentar el resultado del plan de seguridad propuesto, sincronizar las acciones con otras autoridades e informar las necesidades de material, equipo, personal y recursos complementarios dirigidos a garantizar el logro de los objetivos definidos en la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio.

El seguimiento y gestión diario de riesgos, amenazas y desafíos corresponde a cada uno de los comandantes de unidades militares, policiales y responsables de la seguridad en los puntos asignados; sin embargo, el liderazgo municipal y departamental, acompañado por los respectivos secretarios de seguridad, jefes de planeación o sus equivalentes, deberán convocar como mínimo una reunión trimestral de análisis de las condiciones de seguridad, verificando así mismo, los avances respecto a los requerimientos realizados por las autoridades previamente relacionadas.

De igual manera, el liderazgo civil presentará los avances de las gestiones adelantadas para incrementar la cobertura de comunicaciones y conectividad con el ciberespacio en su territorio, así como los proyectos en desarrollo o que se esperan iniciar durante los próximos meses.

Finalmente, el liderazgo civil ejercido con la respectiva Unidad de Gestión del Riesgo municipal o departamental, las entidades, instituciones y las autoridades militares,

Revista Aeronaútica Fuerza Aérea Colombiana

policiales y de seguridad, considerando las condiciones propias del terreno en su área de responsabilidad, efectúan la evaluación del estado de cobertura de las comunicaciones y conectividad en algunos sectores (verde, amarillo y rojo), con las capacidades existentes en su área de responsabilidad y/o jurisdiccional.

A su vez, deberán planear de manera conjunta, coordinada e interagencial y ejecutar al menos una vez por semestre un ejercicio de respuesta a una situación crítica que se pueda presentar en su territorio (siempre en sitios diferentes y distantes), para verificar las coberturas reales de comunicaciones y conectividad, así como para practicar el uso de medios alternos en caso de presentarse fallas en la red de comunicación considerada como principal, para de esta manera poder extractar lecciones aprendidas que permitan identificar necesidades de fortalecimiento, procedimientos y capacidades para posteriormente desarrollar acciones que permitan mitigar o tener superada una falencia al momento de ocurrir un evento real.

3.2.4 Articulación y sincronización de proyectos públicos y privados

Figura 15. Elementos de la articulación y sincronización de proyectos públicos y privados

ARTICULACIÓN Y SINCRONIZACIÓN DE PROYECTOS PÚBLICOS Y PRIVADOS	
Armonización del Plan de Desarrollo Nacional, Planes Sectoriales, Departamentales y Municipales	**Diseño y contribución a la arquitectura de redes de comunicación y conectividad con el ciberespacio**
Seguimiento periódico al avance % cobertura planeados	**Investigación, desarrollo, Innovación I+D+I**
Presupuesto	**Desarrollo del Talento Humano**
Respaldo jurídico	**Ciencia y tecnología: actualización permanente**

Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente al eje estratégico de articulación y sincronización de proyectos públicos y privados.

Articular y sincronizar los proyectos públicos y privados es importante porque reduce la atomización de recursos y esfuerzos, lo que mejora la funcionalidad, el impacto y, durante su implementación, también permite la aplicación práctica de un sistema institucional adaptado a las necesidades de los beneficiarios potenciales de los proyectos. Este enfoque crea oportunidades de coordinación dentro y entre los organismos nacionales.

Por otra parte, la articulación de proyectos impulsa que se utilicen eficientemente los recursos al evitar el gasto desproporcionado en proyectos que no logran el impacto mínimo requerido para alcanzar los objetivos.

A través de la Ley 1341 de 2009 o Ley TIC cuya promulgación tiene como objetivo, de acuerdo con el artículo primero, establecer el marco que permita la definición de las políticas públicas, el régimen de competencia, la protección al usuario, la cobertura y la calidad del servicio (Ley 1341 de 2009). Para ello, se articula con el sector privado que cuenta con los medios y recursos para la cobertura y por su parte, el Estado, dispone de las regulaciones necesarias exigidas como cualquier servicio público para que no se presente abuso de la posición dominante. La Ley de las TIC se promulgó en el 2009, no obstante; la dinámica producida por las necesidades de conectividad ha generado que el año anterior se promulgara la Ley 2108 (2021) en la cual se define que el servicio de internet se constituye en un servicio público esencial.

- **Armonización del plan de desarrollo nacional, planes sectoriales, departamentales y municipales**

La armonización entre estos instrumentos es significativa porque aporta a la formulación, ejecución y evaluación de políticas públicas desde el orden nacional, en las que se incluyan las necesidades específicas de los territorios y de los sectores. Además, la armonización de estos planes beneficia la eficiencia en el gasto, pues las metas territoriales y sectoriales estarían en el mismo sentido que las metas nacionales, lo cual facilita su cumplimiento. Cabe destacar que, según la Ley Orgánica del Plan de Desarrollo, los planes de este nivel que se han propuesto desde las entidades territoriales, buscan

Mejora la funcionalidad, el impacto y, durante su implementación, también permite la aplicación práctica de un sistema institucional adaptado a las necesidades de los beneficiarios potenciales de los proyectos.

no incidir en su autonomía y ajustarse a las políticas y estrategias que integran el Plan Nacional de desarrollo cumpliendo los criterios básicos para que sea coherente frente a los demás contextos normativos.

- **Diseño y contribución a la arquitectura de redes de comunicación y de conectividad con el ciberespacio**

Los diagnósticos integrales de cobertura de comunicaciones y conectividad con el ciberespacio realizados a nivel municipal tanto en el área urbana como veredal, a nivel departamental y nacional, para determinar los mapas de calor (verde, amarillo y rojo) en los territorios, sumado a los ejercicios de verificación, considerando los eventos reales ocurridos y necesidades del país, referencias e insumos para que desde el nivel central, el Ministerio de Tecnologías de la Información y las Comunicaciones o su equivalente encargado diseñar la arquitectura de redes de transmisión de voz y datos y la conectividad, alcance el estado final deseado para el país, pueda planear la ubicación física en el territorio de la infraestructura crítica relacionada, las rutas de distribución de señales o tecnologías y medios alternos que pueden ser utilizados para superar las fallas de cobertura debido a las condiciones propias del terreno o limitaciones tecnológicas existentes en las regiones y los territorios.

Finalmente, el Estado, MinTIC, los gobiernos departamentales, municipales y en general el liderazgo militar, policial

y civil, deben tener presente que si bien es prioritario asegurar la cobertura de comunicaciones y conectividad en los centros más poblados o donde se encuentra la población, de igual manera, por motivos de seguridad nacional es prioritario asegurar la cobertura en áreas consideradas espacios vacíos, los cuales teniendo en cuenta aspectos geoestratégicos y geopolíticos, pueden representar un interés para las comunidades, competidores y actores malignos, razón por la cual las Fuerzas del Estado deben estar preparadas y listas para actuar en estas zonas.

- **Seguimiento periódico al avance porcentual de las coberturas planeadas**

Los planes de acción municipales, departamentales y nacionales, derivados de las estrategias planeadas en los niveles respectivos, fundamentados en aspectos jurídicos y considerando limitaciones presupuestales y logísticas, así como restricciones legales para un período determinado, deben considerar el porcentaje de avance esperado en una línea de tiempo establecida para el fortalecimiento de las tecnologías de la información y comunicaciones en su territorio, contando con capacidades multiespectrales, multidominio, redundantes, complementarias o alternas.

Los gobiernos de turno, el liderazgo militar, policial y civil deberán realizar reuniones periódicas (trimestrales) y ejercicios (semestral) conjuntos, coordinados e interagenciales, para verificar el avance de lo planeado y ajustar los planes de acuerdo con las lecciones aprendidas y según corresponda, buscando que su territorio tenga cobertura plena con sistemas redundantes, alternos y con calidad de señal confiable.

- **Investigación, desarrollo, innovación I+D+I**

Considerando las capacidades del Estado, el conocimiento y experiencia obtenida a través de la evolución y renovación tecnológica permanente, los recursos invertidos en capacitación del talento humano y destinados a centros de investigación y desarrollo, la misión asignada al Ministerio de Tecnologías de la Información y Comunicaciones, así como al Ministerio de Defensa Nacional, las Fuerzas Militares y Policía Nacional, adicionado a la responsabilidad social de las empresas, se identifican necesidades para motivar y gestionar la articulación entre el Estado, la universidad, centros de investigación, desarrollo e innovación tecnológica y empresas de tecnología, para acompañar el diagnóstico de coberturas electromagnéticas en la región, de acuerdo con las capacidades tecnológicas existentes y necesarias para recomendar las rutas más eficientes de transmisión de voz y datos; e igualmente incentivar la generación de productos tecnológicos y desarrollo de software aplicables o

Revista Aeronaútica Fuerza Aérea Colombiana

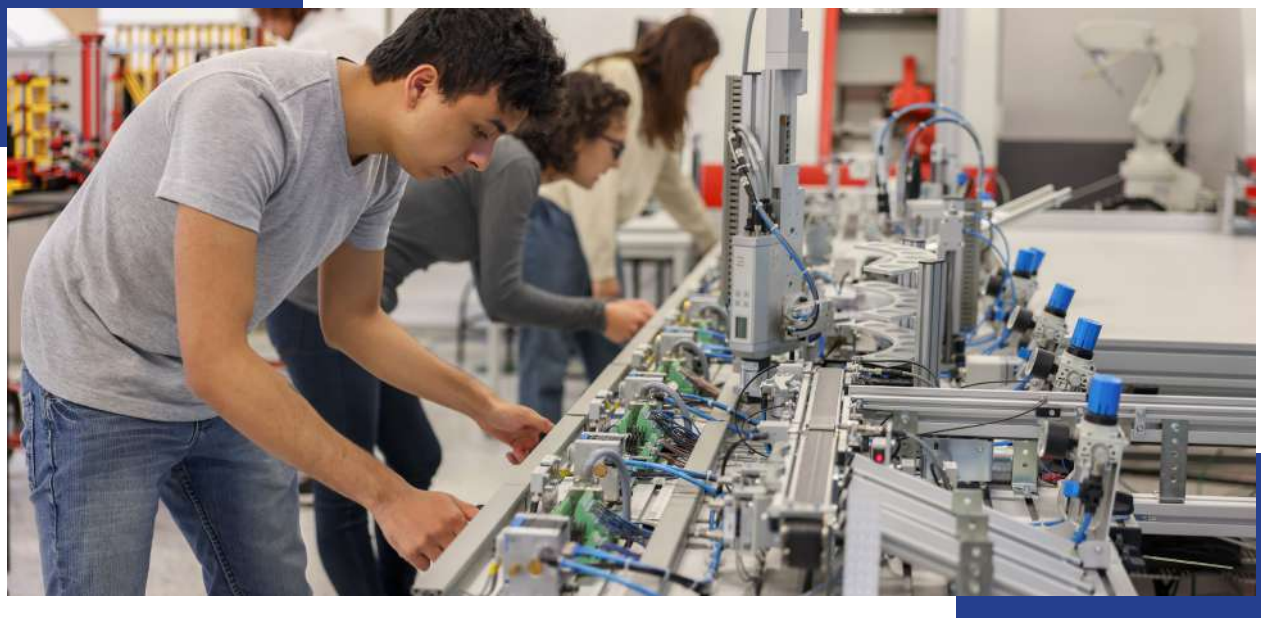
patentables (para sistemas principales o alternos) que permitan resolver problemas específicos, ofreciendo autonomía y autosuficiencia al país respecto a otros actores estatales cuando fuere necesario.

En concordancia con lo expuesto, el Gobierno nacional, departamental y municipal en coordinación con el liderazgo militar, civil y empresarial, debe propender para que el personal de sus regiones (estudiantes, docentes o ciudadanos), militares y policías que se encuentran en las escuelas de formación o centros de investigación científica, se articulen y hagan parte de los diferentes semilleros, grupos y centros de investigación públicos o privados del orden nacional y regional, que tienen capacidades diferenciales complementarias y pueden contribuir a la generación del conocimiento, experimentación, desarrollo de productos tecnológicos y de software aplicables y patentables, considerando siempre, la necesidad de fortalecer los protocolos de seguridad, implementar los formatos de promesa de reserva, compartimentar y manejar de manera limitada la información a quienes cuentan con los niveles correspondientes de seguridad y tienen la necesidad de saber.

- **Presupuesto**

Parte del presupuesto general de la nación debe destinarse a fortalecer las tecnologías de la información y comunicaciones y la conectividad con el ciberespacio; su gestión se hace inicialmente a través del MinTIC, que verifica los proyectos departamentales y municipales a ejecutar en los diferentes planes de acción, a fin de que esa institución alinee, priorice y valide su ejecución, entendiendo que debe ser una entidad dinamizadora para las regiones que buscan alcanzar los objetivos propuestos relacionados con la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio.

Los presupuestos a gestionar deben contemplar aspectos relacionados con el mantenimiento de los equipos y sistemas existentes *(Hardware/ Software),* al igual que la reposición de los mismos, la adquisición de sistemas redundantes y complementarios, así como los recursos necesarios para capacitar y entrenar el talento humano, sin descartar aquellos necesarios para adelantar estudios relativos a la cobertura electromagnética y ejercicios prácticos conjuntos, coordinados e interagenciales sobre el terreno en los cuales se verifique coberturas y funcionamiento de equipos multiespectrales y multidominio, considerados principales y alternos.



- **Desarrollo del talento humano**

La preparación y actualización de las nuevas generaciones es un punto fundamental en la construcción de conocimiento, para que se desempeñen de una forma óptima en torno a la gestión tecnológica y relativa a la conectividad con el espacio y ciberespacio. El conocimiento apropiado, sumado a la experiencia proporcionan la idoneidad requerida para la gestión, preparando el terreno para la construcción del futuro deseado.

El Estado debe cumplir su compromiso frente al desarrollo de un sistema educativo masificado y estandarizado, en el que no se obvien otros énfasis que se quieran abordar y en el que desde edades tempranas se relaciona a los niños y a la juventud con las tecnologías y sus tendencias, enfatizando especialmente en temas como la ciencia, tecnología, ingeniería y matemáticas.

El conocimiento desde tempranas edades, la experimentación en campos tecnológicos, la participación en semilleros, grupos y centros de investigación en los que se materializa el conocimiento en productos desarrollados, aplicables y patentables, contribuye al fortalecimiento de la nación y sus capacidades, consiguiendo autosuficiencia en diversas áreas y campos. De igual manera, la posibilidad de fortalecer el conocimiento y buenas prácticas del talento humano con las que ya cuenta el país, consolidadas a través de convenios entre universidades, centros tecnológicos y empresas tanto al interior del país como en el exterior, en temas relacionados con las tecnologías de información y comunicaciones, así como de conectividad con el ciberespacio, la actualización del conocimiento, comparar lo que se tiene, conocer las tendencias y los procedimientos que se siguen, la tecnología que se utiliza y proponer nuevas opciones para la solución de los problemas actuales o que pueden manifestarse en un futuro.

- **Respaldo jurídico**

El respaldo jurídico opera en dos vías, frente al derecho de los asociados y del Estado como proveedor del servicio público esencial de conectividad. El respaldo jurídico permite tener un piso sólido en relación con este tema, ya que proporciona la certeza de que no se vulneran los derechos de autor o propiedad intelectual, regulando el comportamiento de los actores en el ciberespacio, contribuyendo a que la inversión extranjera se sienta segura y apueste por traer recursos y tecnología al país.

- **Ciencia y tecnología: actualización permanente**

El desarrollo y evolución tecnológica que se ha presentado a través de de la historia de la humanidad generan disrupciones que inciden en la forma como se hacen

las cosas en un espacio de tiempo determinado; pasando de un crecimiento lineal constante, lento y progresivo a un crecimiento constante, exponencial, dinámico con la particularidad que se puede desactualizar rápidamente.

En estas nuevas dinámicas y realidades, implican el seguimiento métodos científicos de estudio y análisis para aprovechar el conocimiento existente, las lecciones aprendidas, y gestionar las acciones a tomar que propicien la rápida implementación para evitar o mitigar cualquier situación que altere el normal funcionamiento de las Redes de Comunicaciones y Conectividad con el Ciberespacio, u otras situaciones, dependiendo de los momentos históricos y realidades tecnológicas de la época.

3.3 Responsables

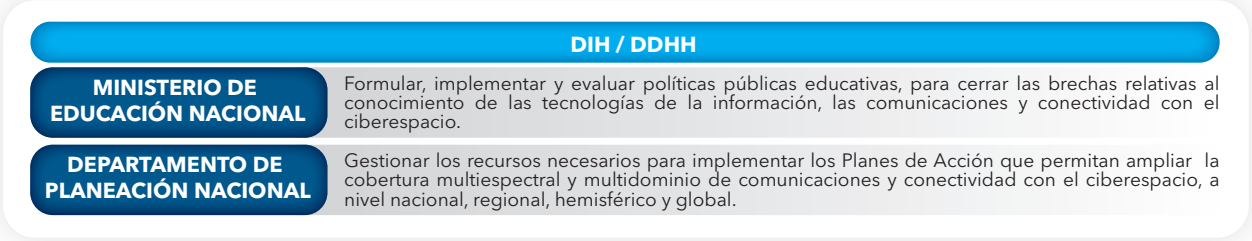
Figura 16. Instituciones responsables en la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio

RESPONSABLES	
ESTADO COLOMBIANO	El liderazgo civil del Estado colombiano, el Ministro de las Tecnologías de la Información y las Comunicaciones y los líderes del Gobierno nacional, departamental y municipal tienen la responsabilidad principal de generar e implementar las políticas, lineamientos y planes de acción que se deriven de la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio, además de gestionar los recursos que se precisan para los estudios y la ejecución de proyectos dirigidos al fortalecimiento de la cobertura multiespectral y multidominio de comunicaciones y conectividad del territorio colombiano, sobre las áreas de interés y más allá de las fronteras; buscando principalmente un desarrollo articulado y sincronizado entre entidades e instituciones del país, el liderazgo militar y policial, la empresa privada y en general, con todos los ciudadanos colombianos que se interrelacionan a nivel nacional, regional, hemisférico y global
GOBIERNO NACIONAL	
MinTIC	
EMPRESA PRIVADA	
FF.MM.	
PNC	
CIUDADANOS	

Fuente: Elaboración propia

3.4 Gestiones contributivas y otras consideraciones

Figura 17. Gestiones contributivas relacionadas con DIH/ DDHH



Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente a las Gestiones contributivas relacionadas con DIH/ DDHH.

Durante el planeamiento y ejecución de los diferentes proyectos estratégicos y planes de acción relacionados con la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio, tiene un lugar de especial importancia el respeto por los Derechos Humanos y el Derecho Internacional humanitario.

De acuerdo con la estrategia corresponde al Ministerio de Educación Nacional, formular, implementar y evaluar las políticas públicas educativas, que permitan cerrar las brechas relativas al conocimiento de las tecnológicas de la información, las comunicaciones y conectividad con el ciberespacio, fomentando alianzas estratégicas que contribuyan al crecimiento exponencial del conocimiento en el talento humano disponible y requerido para desenvolverse en áreas científicas, tecnológicas, de ingeniería y matemática.

Corresponde al Departamento de Planeación Nacional gestionar los recursos que posibiliten la implementación de los planes de acción que permitan ampliar la cobertura multiespectral y multidominio de comunicaciones y conectividad con el ciberespacio, a nivel nacional, regional, hemisférico y global.

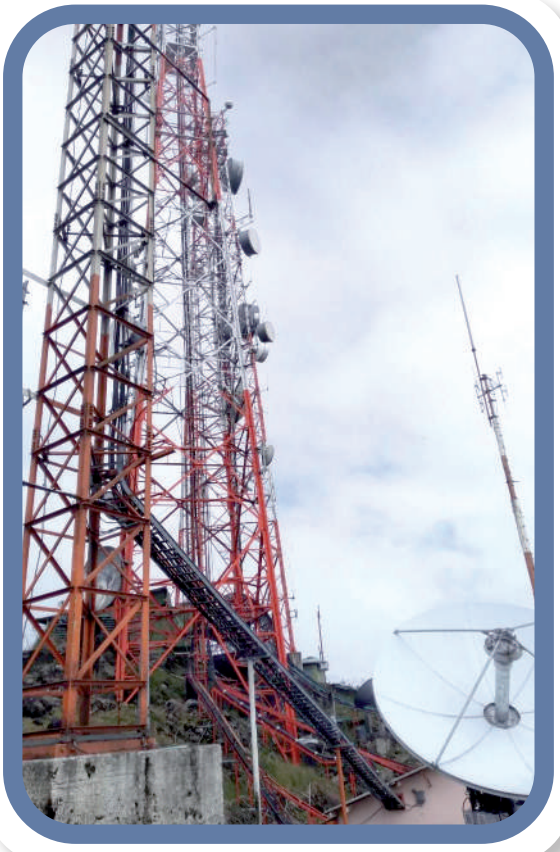
Fomentando alianzas estratégicas que contribuyan al crecimiento exponencial del conocimiento en el talento humano disponible y requerido para desenvolverse en áreas científicas, tecnológicas, de ingeniería y matemática.

3.5 Otras consideraciones

Los actores del orden nacional, departamental o municipal a quienes se les asigne la responsabilidad de implementar o continuar las acciones dirigidas al fortalecimiento de la cobertura de comunicaciones en el país y fuera de él, considerando también la necesidad de gestionar y articular las medidas requeridas en seguridad que mitiguen los riesgos, amenazas y desafíos que tiene la infraestructura crítica relacionada, tanto en la parte física *(hardware)* o intangible *(software)* y puede afectar su normal funcionamiento; deben tener en cuenta así mismo:

1. Difundir la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio en todos los niveles organizacionales pertinentes, considerando los objetivos estratégicos, líneas de acción y ejes estratégicos que deben tener presente el Estado, los líderes militares, policiales y civiles, y en general aquellos actores interesados a nivel nacional, departamental y municipal, a quienes se les asigne la responsabilidad de gestionar la capacidad de comunicación multidominio y multiespectral en el 100 % del territorio y más allá de las fronteras.

2. Analizar el listado consolidado de los riesgos, amenazas y desafíos presentados de manera general en la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio para ajustarlo y complementarlo de acuerdo con las condiciones propias del terreno en su región, las tecnologías existentes y medidas de seguridad implementadas, a fin de ajustar y construir los respectivos planes de acción municipales, departamentales o del orden nacional.



3

Proponer las acciones que deben ser consideradas por el Gobierno nacional, departamental, municipal y actores interesados, al momento de elaborar un plan de acción con el cual se articule y sincronice las entidades tanto públicas como privadas del orden nacional e internacional, para asegurar la capacidad de transmisión y recepción de voz y datos de la nación, así como para interconectarse a través del espacio y ciberespacio a nivel nacional, regional, hemisférico y global.

4

Proponer las acciones que deben ser consideradas por el Gobierno nacional, departamental, municipal y actores interesados, al momento de elaborar un plan de acción con el cual se articule y sincronice las entidades tanto públicas como privadas del orden nacional e internacional, para proteger de amenazas antrópicas y naturales las redes usadas para la transmisión y recepción de voz y datos de la nación, así como su capacidad de interconexión a través del espacio y ciberespacio.

5

Proponer la actualización, modificación, creación o implementación de políticas públicas que articulen y sincronicen la acción unificada del Estado para asegurar y proteger tanto la comunicación y transmisión de voz y datos, así como la infraestructura crítica relacionada.

6

Proponer que el liderazgo civil, militar y policial del orden nacional, departamental y municipal, implementen planes de acción, herramientas y mecanismos que permitan periódicamente verificar y evaluar el estado de la cobertura de comunicaciones y conectividad en el territorio de interés, así como la infraestructura crítica relacionada en su área de responsabilidad, a fin de materializar las acciones necesarias de protección y que permitan dinamizar el alcance de los objetivos propuestos.

7

Proyectar y desarrollar infraestructuras robustas, redundantes y complementarias relativas a las tecnologías de la información y comunicaciones, así como para la conectividad con el ciberespacio, que cuenten con medidas de protección apropiadas para evitar su interrupción, interceptación y/o manipulación por parte de competidores y actores malignos en general.

8

Que el liderazgo militar, policial y civil, del orden nacional, departamental y municipal, continue fortaleciendo el conocimiento y gestionando la actualización del talento humano en los campos relativos a las tecnologías de la información y comunicaciones multiespectrales y multidominio, así como en temas del espacio, ciberespacio, tecnológicos y científicos que motiven la investigación, desarrollo e innovación en estos campos.

9

Entender que las tecnologías de la información y comunicación, así como la conectividad con el ciberespacio son fundamentales para el Gobierno nacional en su arte y manera de gobernar, y así avanzar en el objetivo de lograr un progreso económico, social e institucional que se prolongue y materialice a través de un equilibrio entre el Estado, la sociedad civil y el mercado de la economía (definición de gobernanza de acuerdo con la Real Academia de la Lengua Española).

10

Proponer la creación de un órgano institucional en el nivel estratégico, que permita una gobernanza plena y articulación de proyectos relacionados a nivel municipal, departamental, nacional e internacional, privilegiando la investigación, desarrollo e innovación en los campos de las tecnologías de la información y comunicaciones, así como para la conectividad con el ciberespacio.

11 Mantener un monitoreo permanente de la normatividad legal vigente, la necesidad de actualización e implementación de esta, de otros asuntos legales y jurídicos relacionados.

12 Hacer seguimiento a los avances de los proyectos institucionales y en alianzas público-privadas.

13 El establecer de manera interagencial, conjunta y coordinada procedimientos y mecanismos que permitan una rápida respuesta para el restablecimiento de las comunicaciones y conectividad en un área determinada que pueda estar afectada o sobre la cual por diversos motivos sea necesario actuar.

14 Propender por el desarrollo de planes de acción y proyectos que faciliten la interoperabilidad entre el liderazgo civil, las Fuerzas Militares, policiales, empresa privada y población en general.

15 Dar cumplimiento al Decreto 612 de 2018 que fija a nivel nacional las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del Estado.

OBJETIVOS Y LÍNEAS DE ACCIÓN ESTRATÉGICAS

CAPÍTULO 4

Con el ánimo de alcanzar el "estado final deseado" que propone el "Tener un país con las capacidades tecnológicas necesarias, multiespectrales y multidominio, actualizadas de acuerdo con los momentos evolutivos propios de las tecnologías de la información y comunicaciones; robustas, redundantes y complementarias, protegidas de riesgos, amenazas y desafíos antrópicos o naturales, de rápida recuperación del servicio ante una afectación, que permitan en todo momento de manera confiable y segura, transmitir y recibir voz y datos, así como la interrelación e interconexión a través del espacio y ciberespacio a nivel nacional, regional, hemisférico y global"; se establecen tres objetivos y seis líneas de acción a gestionar, las cuales se presentan y describen a continuación:

Figura 18. Objetivos y líneas de acción estratégicas - Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio

Nota. La figura es un extracto de lo expuesto dentro de la estrategia de seguridad para las redes de comunicación nacional y la conectividad con el ciberespacio apuntando principalmente en los objetivos y líneas de acción estratégicas.

Figura 19. Objetivos estratégicos

01

OBJETIVO ESTRATÉGICO

Garantizar la capacidad de la nación para transmitir y recibir voz y datos, así como para interconectarse a través del espacio y ciberespacio a nivel nacional, regional, hemisférico y global.

La disponibilidad permanente de redes de comunicación multidominio, multiespectrales y de conectividad con el ciberespacio son esenciales para facilitar los procesos relativos a la gobernanza del Estado, con los cuales gestiona la seguridad, las acciones que contribuyen al crecimiento económico, desarrollo y bienestar de la nación, en la dinamización de los principios constitucionales.

Artículo 1

Colombia es un Estado social de derecho, organizado en forma de República unitaria, descentralizada, con autonomía de sus entidades territoriales, democrática, participativa y pluralista, fundada en el respeto de la dignidad humana, en el trabajo y la solidaridad de las personas que la integran y en la prevalencia del interés general (Constitución Política de Colombia, 1991).

Artículo 2

Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares (Constitución Política de Colombia, 1991).

Colombia ha venido fortaleciendo sus relaciones con países amigos, aliados y organismos internacionales de carácter multilateral, de acuerdo con los intereses nacionales en diferentes campos; es importante planear y anticipar las acciones necesarias que permitan mantener una comunicación oportuna, positiva, fluida, confiable, segura las 24 horas del día, con la cual se favorezca la interrelación a nivel nacional, regional, hemisférico y global.

En temas relativos a la Defensa y Seguridad de la nación, el contar con una capacidad de comunicaciones y para la transmisión y recepción de voz y datos, facilita el cumplimiento de la misión definida en el artículo 217 a las Fuerzas Militares constituidas por el Ejército, la Armada y la Fuerza Aérea, cuya "finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional" (Constitución Política de Colombia, 1991, Art. 217).

En el mismo sentido, la Policía Nacional establecida como "un cuerpo armado permanente de naturaleza civil, a cargo de la nación" (Art.218), y que tiene como fin "el mantenimiento de las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz" (Art. 218) puede, con el apoyo de estas herramientas, conseguir esos objetivos definidos en la carta política y que le comprometen junto con las otras fuerzas para cumplir los fines del Estado.

Para garantizar que el país disponga de la capacidad para comunicarse internamente y con el exterior, no solo requiere del despliegue tecnológico, ya que también precisa de medidas de seguridad que como ya se dijo, no se limiten únicamente al mantenimiento y fortalecimiento de las tecnologías existentes, sino que también incluya la ejecución de diagnósticos permanentes respecto a las metas de cobertura y confiabilidad de las comunicaciones.

El desarrollo de estudios sobre las tecnologías más pertinentes y proyecte los recursos correspondientes; considerando la instalación y ubicación de barreras físicas y medidas de seguridad permanente que protejan la infraestructura crítica instalada a nivel local en los municipios (casco urbano y zonas veredales) y departamentos, que al ser afectados inciden en la capacidad de comunicación utilizando el ciberespacio y a través de diferentes medios en todos los ámbitos del país.

Adicionalmente, se debe contemplar en estos planes la capacidad de comunicación y conectividad con los territorios extracontinentales (islas, cayos, u otros existentes en la actualidad o futuro de acuerdo con las circunstancias propias del momento e intereses nacionales definidos).

02

OBJETIVO ESTRATÉGICO

Proteger de amenazas antrópicas y/o naturales las redes usadas para la transmisión y recepción de voz y datos de la nación; así como su capacidad de interconexión a través del espacio y ciberespacio.

La Oficina de Coordinación de Asuntos Humanitarios de la Organización de las Naciones Unidas (OCHA) (2014), define la amenaza antrópica, como:

> aquel peligro latente generado por la actividad humana en la producción, distribución, transporte y consumo de bienes y servicios, y la construcción y uso de infraestructura y edificios. Comprende una gama amplia de peligros como lo son las distintas formas de contaminación de aguas, aire y suelos, los incendios, las explosiones, los derrames de sustancias tóxicas, los accidentes en los sistemas de transporte, la ruptura de presas de retención de agua etc. (Oficina para la Coordinación de Asuntos Humanitarios, 2014)

Considerando las circunstancias propias del momento en las cuales se han identificado intereses de Estados opositores y actores malignos como grupos terroristas, delincuencia organizada, grupos del crimen organizado transnacional, de la delincuencia común, entre otros no determinados, que recolectan información relacionada con la infraestructura crítica y las capacidades de la nación en diferentes campos para en algún momento atentar contra esta, observando necesidades en el ajuste y fortalecimiento de las medidas de seguridad para evitar que el normal funcionamiento del país y capacidad para comunicarse de manera regular o en situaciones de crisis sea afectada.

El Estado debe tener la capacidad para disponer de manera inmediata, ante una situación de crisis, los medios y recursos necesarios que, articulados a través de la Unidad Nacional de Gestión del Riesgo (UNGR), conformen un sistema de comunicaciones eficiente, confiable y disponible las 24 horas del día, con cobertura plena sobre el territorio nacional o más allá de donde sea requerido (Unidad Nacional de Gestión del Riesgo, 2017)

Al precisar el significado del término "natural", de acuerdo con lo definido por la UNGR (2017), cabe decir que se refiere a una amenaza en la participan las personas, construyéndose en un "evento físico, como, por ejemplo; una erupción volcánica que no afecta al ser humano es un fenómeno natural y no una amenaza natural" (Organización de Estados Americanos, s.f.).

Por otro lado, en lo que respecta a las amenazas la Organización de Estados Americanos afirma que cuando un fenómeno natural se presenta en un área poblada se establece como un suceso peligroso que puede causar fatalidades y daños que superan la capacidad de respuesta de la sociedad y se identifica como desastre natural.

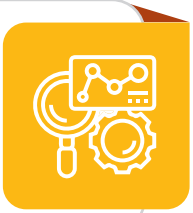
En las áreas donde no se encuentran intereses humanos, no se considera que los fenómenos naturales sean amenazas y tampoco se categorizan como desastres, diferenciándose del concepto común en el que desastres naturales se perciben como estragos inevitables que propician las fuerzas de la naturaleza cuando se salen de control. Además, un desastre no solo se deriva de un proceso netamente natural, ya que es un evento que se presenta en lugares en donde se desarrollan actividades humanas. (Organización de Estados Americanos, s.f.)

En los fenómenos naturales potencialmente peligrosos y que pueden afectar directa o indirectamente las capacidades de la nación para comunicarse e interrelacionarse a nivel interno y externo por diversos medios, canales y ámbitos (terrestre, marítimo, fluvial, aéreo, espacial, ciberespacial, cognitivo) se encuentran los atmosféricos (granizo, huracanes, incendios, tornados, tormentas tropicales), hidrológicos (inundación costera, desertificación, salinización, sequía, erosión y sedimentación, desbordamiento de ríos, olas ciclónicas, olas en cuerpos de agua seiches), volcánicos (fragmentos pequeños de ceniza y lava denominados tefra y lapilli, gases, flujos de lava, corrientes de fango, explosiones laterales y proyectiles generados, flujos piro plásticos), incendios (matorrales, bosques, pastizales, sabanas) y geológicas-hidrológicas (avalanchas de ripio, suelos expansivos, deslizamientos, desprendimiento de rocas, deslizamientos submarinos, hundimiento de tierra) (Organización de Estados Americanos, s.f.)

03

OBJETIVO ESTRATÉGICO

Realizar un diagnóstico para la gestión permanente del estado de las redes de comunicación nacional y de conectividad con el ciberespacio.



El diagnóstico del estado actual de la infraestructura crítica existente en el país relativa a redes de comunicación nacional y conectividad con el ciberespacio, así como su correlación con tecnologías utilizadas en el mundo, es fundamental para el planeamiento y ejecución de una acertada estrategia.

La pertinencia y vigencia de los procedimientos operacionales actuales, la funcionabilidad de las tecnologías en uso que están proyectadas para ser aprovechadas en el corto, mediano y largo plazo, así como la cobertura y redundancia de comunicaciones multidominio dentro y fuera del territorio nacional, la gestión de riesgos, amenazas y desafíos junto con la sincronización acompañada de la articulación de proyectos públicos y privados relativos al asunto contribuyen directamente a alcanzar el estado final deseado.

La estrategia de seguridad para las redes de comunicación y la conectividad con el ciberespacio, establece seis (06) líneas de acción estratégicas que contribuyen directamente para alcanzar los objetivos propuestos; las principales consideraciones y acciones a gestionar se presentan a continuación:

Figura 20. Líneas de acción estratégicas

01 LÍNEA DE ACCIÓN ESTRATÉGICA

Políticas, lineamientos, normatividad y marco legal vigente acorde a las necesidades del momento.

Es fundamental establecer y emitir políticas, normatividad y el marco legal correspondiente de acuerdo a las circunstancias propias del momento, en la estandarización de las acciones legítimas que pueden desempeñar las instituciones públicas y privadas, como marcos de referencia que permitan a empresas e inversores privados, estatales y ciudadanos nacionales y extranjeros, conocer claramente las reglas de actuación en el territorio colombiano y más allá de sus fronteras.

Delimitar el alcance de las acciones en el campo de las tecnologías de la información y comunicación del país, provee un respaldo para el ejercicio de quienes toman decisiones, incluyendo a los servidores públicos, quienes dinamizan los compromisos contemplados en los planes de desarrollo, planes estratégicos institucionales y planes de acción en general; no solamente en términos de gestión, sino en la proyección de los recursos suficientes para satisfacer las necesidades identificadas o para iniciar cuando fuere necesario, las actualizaciones legales disciplinarias, administrativas o penales a que hubiere lugar.

Disponer de políticas y lineamientos claros relacionados con el fortalecimiento de las tecnologías de la información y comunicaciones multidominio y multiespectral para la cobertura del 100% del territorio nacional, así como respecto a la conectividad con el ciberespacio, permite articular las iniciativas desde el nivel central nacional con los niveles departamentales y municipales para alcanzar los objetivos determinados en la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio, maximizando el uso de los recursos estatales destinados al mantenimiento, actualización, adquisición y/o reposición de *hardware* y *software*, así como destinados a la capacitación y actualización del talento humano.

Se debe considerar que los lineamientos vistos como regla, especialmente los emanados por el Ministerio de Tecnologías de la Información y las Comunicaciones, formulan un marco de actuación ético que define hasta dónde un servidor público, contratista privado o ciudadano nacional o extranjero puede llegar, o qué puede y qué no puede hacer en algunas circunstancias.

En el mismo sentido, a pesar de las dinámicas propias de la democracia en la cual se alternan los actores comprometidos en la toma de decisiones, existe una permanencia en el tiempo de las políticas, lineamientos y marcos de actuación, dando continuidad a proyectos que contribuyen a la evolución, desarrollo y crecimiento del país.

La normatividad de referencias para Colombia en relación con las redes de comunicación y conectividad es regida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), impartiendo medidas como el Modelo de Seguridad y Privacidad de la Información (MSPI) contenido en la norma 27001 del 2013, en la que se promueve la implementación de mejores prácticas de seguridad de la información. En este sentido, también se pueden enunciar los documentos CONPES 3701 Lineamientos de política para la ciberseguridad y ciberdefensa, CONPES 3854 Política nacional de seguridad digital y CONPES 3995 Política nacional de confianza y seguridad digital.

Las Fuerzas Militares cuentan con una red integrada de comunicaciones (RIC), de allí la importancia de que en la actualización periódica de la norma 27001 vigente, se reglamente como red alterna la infraestructura de MinTIC en casos críticos de interés nacional para ser empleada por el Ministerio de Defensa Nacional.

02 LÍNEA DE ACCIÓN ESTRATÉGICA

Identificar la infraestructura crítica de la nación necesaria para la transmisión de voz y datos, así como para la conectividad a través del espacio y ciberespacio.

Para el desarrollo de una estrategia integral de seguridad es indispensable tener presente en todo momento que los equipos, medios, recursos principales y de soporte directo e indirecto que hacen parte de los activos relativos a las tecnologías de la información, comunicaciones y conectividad con el ciberespacio, se asuman como parte de la infraestructura crítica de la nación, proporcionando la protección necesaria de acuerdo a los niveles de amenaza, riesgo y vulnerabilidad que les puede afectar de manera potencial o permanente.

Es por esto que las autoridades civiles, militares y policiales en coordinación con la empresa privada y otras entidades tanto nacionales como internacionales, según corresponda, se deben reunir para verificar la capacidad instalada en su territorio, las coberturas del espectro electromagnético, comunicaciones de voz, datos e internet, para actualizar el mapa respectivo que permita identificar claramente las áreas sobre las cuales se debe avanzar en la ampliación de la cobertura en el servicio y la calidad del mismo, buscando principalmente, asegurar la comunicación entre ciudadanos y población ubicada en áreas alejadas de los centros urbanos, anticipar la necesidades de comunicación por parte de las fuerzas de seguridad y el orden en algún momento determinado.

Las autoridades civiles, militares y policiales en coordinación con la empresa privada, deben identificar la ubicación de la infraestructura considerada crítica, la cual al ser afectada podría perjudicar el proceso de comunicación, conectividad con el ciberespacio y/o transmisión de voz y datos para posteriormente gestionar los planes que permitan implementar las medidas de seguridad y protección necesarias.

La Red Integrada de Comunicaciones (RIC) empleada por las Fuerzas Militares de Colombia pertenece a estas instituciones y de ser necesario, se articula con la Policía Nacional para atender situaciones críticas. Por medio de esta se transmiten y reciben voz y datos en forma segura a través del territorio nacional.

La red está integrada por diferentes repetidoras ubicadas en cerros, complementadas con redes de conectividad multiespectrales y multidominio. La RIC al igual que otras capacidades del Estado debe identificarse como infraestructura crítica, protegerse de amenazas físicas, pero también demanda el desarrollo de análisis prospectivos y estudios permanentes que permitan anticipar los cambios tecnológicos y la reserva de recursos para su modernización, evitando que pueda quedar en desuso por obsolescencia, afectando también las capacidades de la nación. Lo mencionado justifica la implementación continua de otros sistemas como los de fibra óptica y nuevas tecnologías que maximicen la velocidad, fidelidad de la señal y capacidad de interconexión en la garantía de una cobertura total.

03 LÍNEA DE ACCIÓN ESTRATÉGICA

Identificar riesgos, amenazas y desafíos relacionados.

Establece necesidades frente a la ejecución de un análisis integral que permita identificar riesgos, amenazas y desafíos clasificados como naturales y antrópicas que afectan o pueden potencialmente perturbar el normal funcionamiento de las redes de comunicación nacional y la conectividad con el ciberespacio. Un levantamiento inicial de información contribuirá al proceso de planeación de la seguridad requerida de acuerdo con la tecnología e infraestructura existente.

En el mismo sentido, siendo conscientes de la limitación de recursos, el tomador de decisiones conforme con las circunstancias propias del momento, podrá priorizar las acciones a ejecutar en un lugar determinado a fin de destinar y distribuir recursos de manera más eficiente.

Hay que considerar que, riesgos, amenazas y desafíos se pueden manifestar de manera física cuando por ejemplo se deteriora, daña o destruye un equipo, parte de un sistema, un componente principal, alterno, de soporte, etc., o también de manera no física cuando se degrada, bloquea, limita, etc. la capacidad del software que permite la gestión de equipos tecnológicos y el uso de manera apropiada de la información gestionada a través de estos.

Es fundamental, así mismo, entender que algunas políticas y lineamientos no se encuentran ajustadas a las realidades y necesidades de la nación abriendo espacios para originar efectos no deseados respecto a la capacidad del Estado para alcanzar los objetivos propuestos relacionados con “garantizar la capacidad de la nación para transmitir y recibir voz y datos; así como para interconectarse a través del espacio y ciberespacio a nivel nacional, regional, hemisférico y global” y “proteger de amenazas antrópicas y/o naturales las redes usadas para la transmisión y recepción de voz y datos de la nación; así como su capacidad de interconexión a través del espacio y ciberespacio”.

04 LÍNEA DE ACCIÓN ESTRATÉGICA

Identificar y articular entidades públicas y privadas de la nación con capacidades apropiadas, para de manera sinérgica proteger y asegurar la infraestructura crítica.

Corresponde al Estado, representado por el Gobierno nacional y específicamente el Ministerio de Tecnologías de la Información y las Comunicaciones, desarrollar las acciones necesarias para sincronizar un plan de acción entre las entidades públicas y privadas con el cual se identifique y priorice la necesidad de protección, y se asegure la infraestructura crítica identificada tanto en el territorio nacional como fuera de él.

La identificación de infraestructura crítica relativa a las redes de comunicación y conectividad con el ciberespacio a la cual se le debe ofrecer seguridad comienza a nivel municipal cuando el alcalde, su oficina de planeación y autoridades militares y policiales tienen una claridad frente a las capacidades físicas existentes no solo en el casco urbano sino en las zonas veredales.

MinTIC debe gestionar de manera integral al Estado para fortalecer alianzas estratégicas con el Ministerio de Defensa Nacional, las Fuerzas Militares, la Policía Nacional y otras entidades e instituciones, así como con la empresa privada tanto nacional como internacional y comunidades donde sea necesario, para luego de identificada la infraestructura a proteger y priorizado su nivel de impacto en caso de presentarse alguna situación que la afecte, determinar los tipos y niveles de protección requeridos, elaborando los planes respectivos que permitan definir las capacidades similares y complementarias que se necesitan.

Un análisis completo e integral desde lo municipal considerando lo veredal y el impacto departamental, nacional e internacional, permitirá la construcción de protocolos de seguridad para la mitigación de amenazas y por ende la construcción de directrices y procedimientos para la reducción de los desafíos detectados.

Todas las organizaciones e instituciones públicas o privadas están obligadas y deben propender por dar cumplimiento a los lineamientos y estándares de la estrategia orientada a garantizar la seguridad de la infraestructura crítica en materia de redes y conectividad creando una sinergia que permita la construcción de una protección efectiva. Una estrategia perfectamente articulada y materializada a través de políticas que sean de obligatorio cumplimiento minimiza las debilidades o desafíos, contribuyendo a promover lineamientos dirigidos a la protección de las redes de comunicación y de conectividad.

05

LÍNEA DE ACCIÓN ESTRATÉGICA

Identificar y gestionar la implementación de tecnologías apropiadas y necesarias para garantizar las comunicaciones y conectividad de acuerdo con la evolución tecnológica y/o circunstancias del momento.

Indudablemente, el desarrollo tecnológico tiene una evolución exponencial; que implica identificar la vida útil de los equipos existentes utilizados para la transmisión de voz y datos a través de redes de comunicación, anticipar las necesidades de mantenimiento, actualización y reposición de estos, para que cada vez tengan mayores capacidades, sean más confiables y seguros al momento de ser utilizados.

Las nuevas tecnologías facilitan mayores coberturas, requieren menos infraestructura y equipos de soporte, sin embargo, los costos de estas pueden ser más elevados, por lo cual debe existir un análisis responsable que permita proyectar en el tiempo la inversión de recursos, maximizando la utilización de estos.

Los roles y responsabilidades para quienes se desempeñan en el ambiente de las comunicaciones y la conectividad están sometidos a condiciones particulares dada la velocidad del cambio y evolución de la tecnología; de ahí la importancia de adaptarse para generar de forma eficaz lineamientos y estrategias que permitan asumir los nuevos retos con celeridad de una forma apropiada.

Es fundamental igualmente, prever la capacitación y actualización permanente del talento humano que se desempeña en estas áreas de conocimiento, quienes además se convierten en actores principales que permiten prevenir y detectar amenazas latentes para una rápida reacción en temas de seguridad.

06

LÍNEA DE ACCIÓN ESTRATÉGICA

Diagnosticar, gestionar y proyectar el estado final deseado.

Reúne los elementos de análisis fundamental con los cuales se materializa el propósito que deben alcanzar los dirigentes del Estado, mediante el desarrollo de acciones para neutralizar y mitigar los riesgos, amenazas y desafíos que pueden afectar el normal funcionamiento del país, su interacción con otras naciones y organismos internacionales de carácter multilateral o su capacidad para responder de manera sincronizada a las situaciones de crisis que se puedan presentar en su área de responsabilidad.

Se orienta a la dinamización de los ejes estratégicos y las acciones que impactan la gestión de las demás líneas de acción y los objetivos estratégicos planteados.

Revista Aeronaútica Fuerza Aérea Colombiana

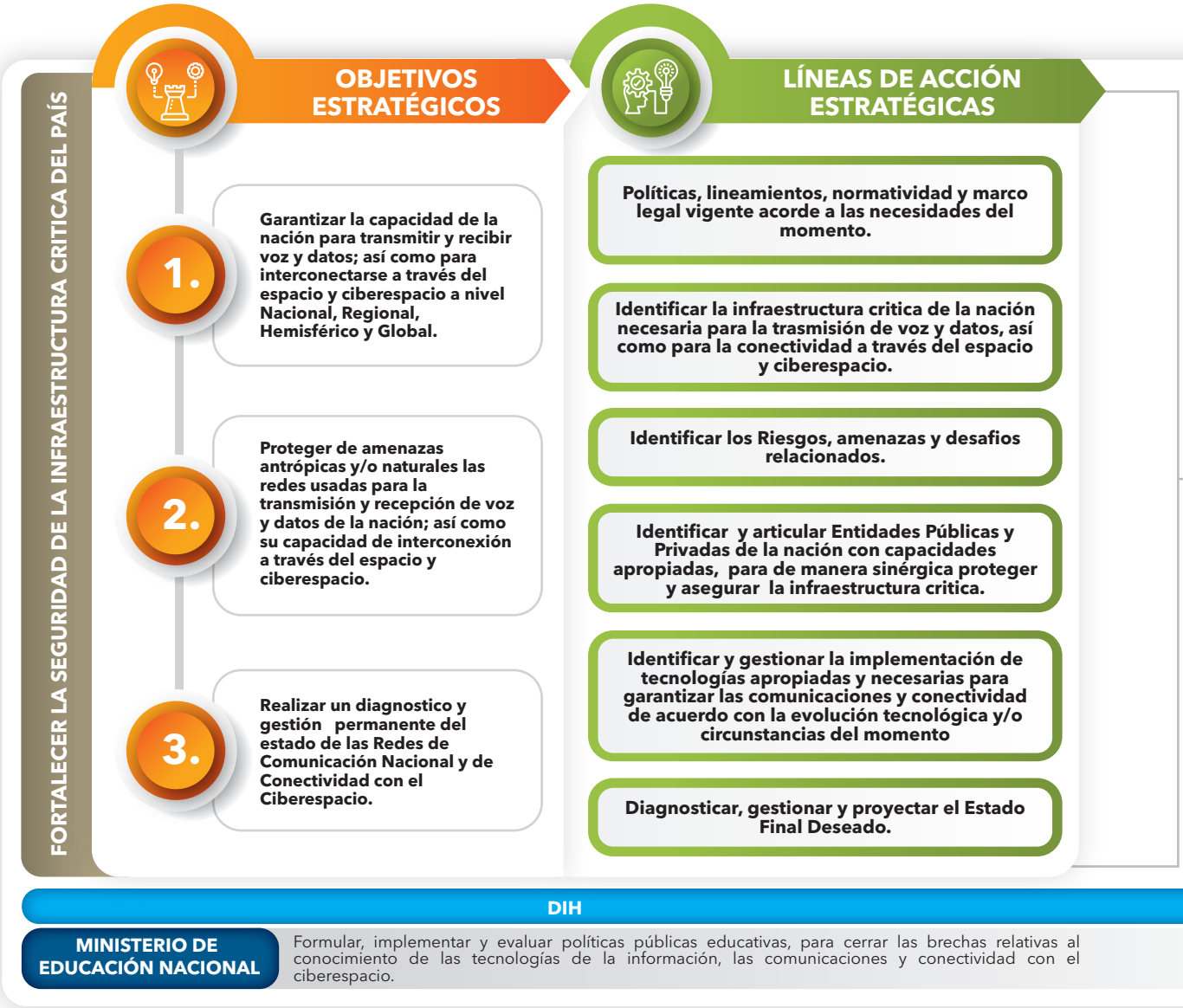

EUR /USD
Open at
Lots
2,5386
3,7762
2,3574
MARGIN 59.25 USD
January
March
April
May
BUY
3,6538
SELL
4,5762
Order
18.73
volume
9.52

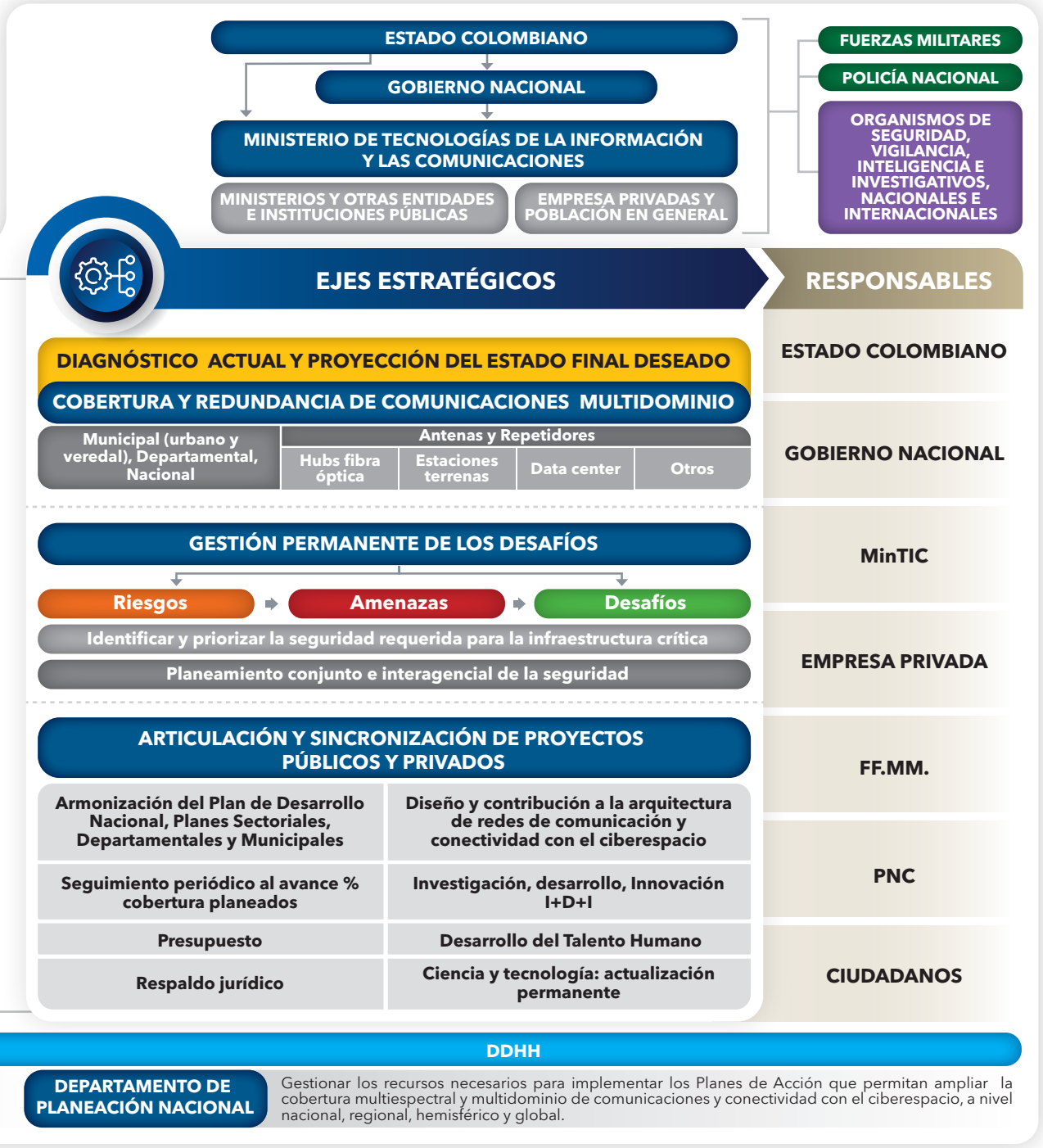
SÍNTESIS DE LA ESTRATEGIA

CAPÍTULO 5

SÍNTESIS DE LA ESTRATEGIA

Figura 21. Representación gráfica de la Estrategia de Seguridad para las Redes de Comunicación Nacional y la Conectividad con el Ciberespacio.





Fuente: Elaboración propia con base en información proporcionada por el grupo de expertos reunido en desarrollo de la materia Estrategia Militar Nacional Aplicada en el curso CAEM-CIDENAL (2022).

REFERENCIAS

Álvarez Calderón, C. E. (Ed.). (2018). *Escenarios y desafíos de la seguridad multidimensional en Colombia*. Sello Editorial ESDEG. Recuperado a partir de https://esdeguelibros.edu.co/index.php/editorial/catalog/book/27

Balleteros, M. Á. (2016). *En busca de una Estrategia de Seguridad Nacional*. (Secretaria General Técnica Ministerio de Defensa, Ed.) https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2016/MABM_ESN.pdf

Comando General de las Fuerzas Militares. (02 de agosto de 2019). *Capacidades Departamento Conjunto de Comunicaciones*. https://www.cgfm.mil.co/es/capacidades-departamento-conjunto-de-comunicaciones

Comando General de las Fuerzas Militares. (02 de agosto de 2019). *Misión Departamento Conjunto de Comunicaciones Fuerzas Militares*. https://www.cgfm.mil.co/es/mision-departamento-conjunto-de-comunicaciones-fuerzas-militares

Constitución Política de Colombia. (7 de julio de 1991). Bogotá, Colombia.

de Motes, J. M. (1992). Los Pioneros de la Segunda Revolución Industrial en España: la Sociedad Española de Electricidad (1881-1894). *Revista de Historia Industria*(2), 121-142. https://core.ac.uk/download/pdf/39047963.pdf

Decreto 1414 de 2017, Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones. (25 de agosto de 2017).

Dirección General - Oficina de Telemática. (2019). *Plan Estratégico de Tecnologías de la Información y las Comunicaciones 2019-2022 "La transformación digital del servicio de policía"*. https://www.policia.gov.co/sites/default/files/descargables/plan_estrategico_de_tecnologias_de_la_informacion_y_las_comunicaciones_-_peti_2019_-_2022_0.pdf

La Guerra en la Historia de la Humanidad. (s.f.). https://avafp.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_50496_1&content_id=_1450260_1

Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional de Espectro y se dictan otras disposiciones (30 de julio de 2009). https://bit.ly/3Rhj1vB

Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres y se dictan otras disposiciones (24 de abril de 2012). https://bit.ly/3fqH9Pe

Ley 2108 de 2021, "Ley de Internet como Servicio Público Esencial y Universal" o "Por medio de la cual se Modifica la Ley 1341 de 2009 y se dictan otras Disposiciones" (29 de julio de 2021). https://bit.ly/3BKmHQB

Ministerio de Defensa Nacional. (diciembre de 2018). *Modelo de Planeación y Desarrollo de las Capacidades de la Fuerza Pública*. https://bit.ly/3SARNkx

Ministerio de Defensa Nacional. (2019). *Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018-2022*. https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/Documentos_Descargables/espanol/PETI2018-2022.pdf

MinTIC. (2022). *Quienes somos*. https://www.mintic.gov.co/portal/inicio/Ministerio/Acerca-del-MinTIC/118042:Quienes-Somos

Oficina de Tecnologías de la Información y las Comunicaciones. (1 de septiembre de 2022). *Misión*. https://www.policia.gov.co/oficinas-asesoras/telematica

Oficina para la Coordinación de Asuntos Humanitarios. (19 de junio de 2014). *Amenaza antrópica*. https://wiki.salahumanitaria.co/wiki/Amenaza_antr%C3%B3pica

Organización de Estados Americanos. (s.f.). *¿Qué son las amenazas naturales?* https://www.oas.org/dsd/publications/Unit/oea57s/ch005.htm

Ramírez, Y. E., Álvarez, C. E., Ruiz, D., Rosanía, N. A., Gómez, J. C., Sánchez, D. P., . . . López, G. (2017). *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia*. (C. E. Álvarez, Ed.) Sello Editorial ESDEG. https://doi.org/https://doi.org/10.25062/9789585652835

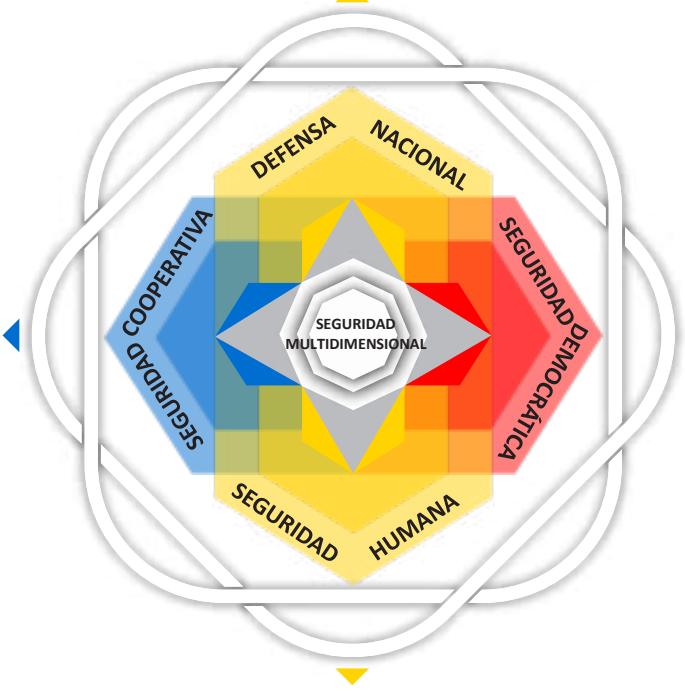
Unidad Nacional de Gestión del Riesgo. (2017). *Terminología sobre gestión del riesgo de desastres y fenómenos amenazantes. https://bit.ly/3dFmjuY*

Vargas, J. E. (abril de 2002). *Políticas Públicas Para la Reducción de la Vulnerabilidad Frente a los Desastres Naturales y Socio-naturales*. https://repositorio.cepal.org/bitstream/handle/11362/5749/S2002612_es.pdf?sequence=1&isAllowed=y

ANEXO

Anexo A. Marco normativo
https://www.mintic.gov.co/portal/715/articles-198952_anexo_1_1_marco_politica_normativo.pdf

Soberanía
Nacional



Problemas
de Seguridad
Comunes

Democracia
participativa
Valor Central

Protección de la
persona
humana

Estrategia de Seguridad
para las

REDES DE COMUNICACIÓN NACIONAL Y LA CONECTIVIDAD CON EL CIBERESPACIO

2022 - 2032

MINISTERIO DE DEFENSA NACIONAL

ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
Colombia

KONRAD ADENAUER STIFTUNG