Actualización de la guía metodológica para la identificación de las infraestructuras críticas cibernéticas de Colombia

Jorge Ernesto Mejía Giraldo
Diego Edison Cabuya Padilla

Trabajo de grado para optar al título profesional:
Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Actualización de la guía metodológica para la identificación de las Infraestructuras Críticas Cibernéticas de Colombia

Alumno:

Jorge Ernesto Mejía Giraldo

Director:

Diego Edison Cabuya Padilla

Grupo de Investigación

Masa crítica

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de grado

Bogotá – Colombia

2020

Ministerio de defensa nacional

Actualización de la guía metodológica para la identificación de las Infraestructuras Críticas Cibernéticas de Colombia

Jorge Ernesto Mejía Giraldo

Ministerio De Defensa Nacional

Comando General Fuerzas Militares

Escuela Superior De Guerra

Maestría En Ciberseguridad y Ciberdefensa

Trabajo de grado para optar el título de Magíster En Ciberseguridad y Ciberdefensa

Bogotá – Colombia

2020

Declaración de originalidad por parte del autor

Mediante la presente certifico que soy el único autor de esta monografía. Todos los materiales usados, referencias de literatura y estudios elaborados por otras personas han sido referenciados en el presente documento. Así mismo este proyecto de grado no se ha presentado para su examen en ningún otro lugar.

Autor: [JORGE ERNESTO MEJÍA GIRALDO]

Resumen

Actualización de la guía metodológica para la identificación de las Infraestructuras Críticas Cibernéticas de Colombia

Las Infraestructuras Críticas Cibernéticas (ICC) son una parte esencial de cualquier IC para llevar a cabo sus procesos y de esta manera poner a disposición de la población los servicios esenciales que estas prestan, mediante la transferencia de información y las telecomunicaciones que componen estos sistemas. A medida que los servicios que se prestan a la sociedad se interconectan entre sí, se incrementa con ello la probabilidad de interrupciones mediante la explotación de vulnerabilidades.

El impacto que genera la incorrecta identificación de los servicios vitales podría ocasionar un efecto en cascada de aquellos servicios y activos críticos que soportan la supervivencia de la población, tales como: el servicio de acueducto, el sistema eléctrico, el sistema de salud, entre otros. Por lo tanto se requiere de políticas y estrategias de ciberseguridad y ciberdefensa, que permitan su protección y de esta manera garantizar su disponibilidad e integridad.

El propósito de este trabajo académico es generar la actualización de la guía metodológica para la identificación de las infraestructuras críticas cibernéticas de Colombia, las cuales se encuentran distribuidas en trece sectores estratégicos, a través de la propuesta de nuevos criterios de criticidad, ellos son: (1) salud pública y seguridad humana, (2) económico, (3) interdependencia, (4) tiempo de recuperación y (5) medioambiente, con los cuales se busca llevar a cabo una mejor priorización de las ICCC, para reducir la vulnerabilidad por causas intencionales, mediante el empleo del ciberespacio. La experiencia ha demostrado que es un

proceso bastante sencillo identificar los activos críticos; sin embargo, a menudo es muy difícil establecer la criticidad de un activo en comparación con otros activos.

La propuesta se ha diseñado para ser presentada al Comando Conjunto Cibernetico, bajo el análisis conceptual de diferentes teorías, estándares y metodologías existentes para la identificación, priorización y catalogación de las Infraestructuras Críticas Cibernéticas (ICC); al igual que del aprovechamiento del conocimiento de diferentes expertos en el país sobre el tema en mención, es así como se plantean que sean llevadas a cabo seis actividades que son consideradas necesarias para la identificación de la ICCC; generando de esta manera la segunda versión de la guía metodológica para la identificación de ICCC, cuya primera versión se publicó en el 2015.

Palabras clave: Infraestructura crítica cibernética, infraestructura crítica, ciberespacio, servicios esenciales, criterios de criticidad.

Abstract

Update of the Methodological Guide for the Identification of Colombian Critical Information Infrastructures.

Cyber Critical Infrastructures (ICC) are an essential part of any IC to carry out its processes and thus make available the essential services they provide to the population, through the transfer of information and telecommunications that make up these systems. Because of services provided to society are interconnected, rise the probability of interruptions by taking advantage of vulnerabilities.

The impact generated by the incorrect identification of vital services could cause a cascading effect of those services and critical assets that support the population survival, such as: aqueduct service, electrical system, health system, among others. Therefore, cybersecurity and cyber defense policies and strategies are required, in order to allow their protection and thus guarantee their availability and integrity.

The purpose of this academic work is to generate the update of the methodological guide for the identification of critical cybernetic infrastructure in Colombia, which are distributed in thirteen strategic sectors, with the proposal of new criticality criteria, they are: (1) public health and human security, (2) economic, (3) interdependence, (4) recovery time and (5) environment, its pursue to carry out a better prioritization of the ICCC, reducing vulnerability by intentional causes, by the use of cyberspace. Experience has shown that it is a fairly straightforward process to identify critical assets; however, it is often very difficult to establish the criticality of an asset compared to other assets.

The proposal has been designed under the conceptual analysis of different theories, standards and existing methodologies for the identification, prioritization and cataloging of

Critical Cyber Infrastructure (ICC); As well as taking advantage of the knowledge of different experts in the country on the subject, it is how that six activities are proposed being carried out in order to identify the ICCC; Thus generating a second version of the methodological guide for the identification of ICCC, version first was published in 2015.

Key words: Critical cyber infrastructure, critical infrastructure, cyberspace, essential services, criticality criteria.

Abreviaciones y términos

ColCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia
CCOCI	Comando Conjunto Cibernético de las Fuerzas Militares
CCP	Centro Cibernético Policial
CONPES	Consejo Nacional de Política Económica y Social
DNP	Departamento Nacional de Planeación
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
IC	Infraestrutura Crítica
ICC	Infraestrutura Crítica Cibernética
ICCC	Infraestrutura Crítica Cibernética de Colombia
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
TI	Tecnologia de la informacion
TIC	Tecnologías de la Información y las Comunicaciones.
TO	Tecnologías de operación

Tabla de contenido.

Introducción. 15

Capítulo I 18

Generalidades del trabajo de investigación. 18

1.1 Descripción del problema. 18

1.2 Justificación e impacto. 21

1.3 Pregunta de Investigación. 25

1.4 Alcance. 25

1.5 Objetivo Principal. 25

1.6 Objetivos Específicos. 25

1.7 Metodología. 26

Capítulo II 29

Infraestructura crítica e infraestructura critica cibernética. 29

2.1 Conceptos básicos. 29

2.2 Conceptos relacionados con la Infraestructura Crítica. 30

2.3 Conceptos relacionados con la Infraestructura Crítica Cibernética. 34

2.4 Sectores de las Infraestructuras Críticas Cibernéticas y su protección. 37

Capítulo III 47

Mejores prácticas en el proceso de identificación de las ICC. 47

3.1 Criterios para determinar las infraestructuras Críticas Cibernéticas. 47

3.2 Análisis de la guía para la identificación de las Infraestructuras Criticas Cibernéticas de Colombia. 49

3.3 Análisis de metodologías para la identificación y priorización de las ICC. 54

3.4 Análisis de los Organismos Involucrados en el Proceso de Identificación de la ICCC .68

3.5 Propuestas de valor para la protección de las ICC, a través de su identificación. 73

Capítulo IV.....76

Identificación de las características, criterios o variables de las ICC. 76

4.1 Necesidad de la actualización de la Guía Metodológica 76

4.3 Criterios para la identificación, catalogación y priorización de la ICCC. 90

4.3.1 Salud pública y seguridad humana. 95

4.3.2 Impacto Económico. 96

4.3.3 Impacto de la Interdependencia de las infraestructuras. 97

4.3.4 Tiempo de recuperación de la infraestructura. 99

4.3.5 Medioambiente. 100

Capítulo V 105

Propuesta de actualización de la guía metodológica para la identificación de ICCC. 105

Conclusiones. 117

Recomendaciones. 120

Referencias. 121

Anexos. 130

Listado de figuras.

Figura 1. Interdependencia entre los sectores. 35

Figura 2. Las Infraestructuras Criticas Cibernéticas. 45

Figura 3. Diagrama de Infraestructura. 50

Figura 4. Marco Metodológico para la identificación de la ICCC. 51

Figura 5. Ilustración de la metodología para la identificación de los servicios críticos. 65

Figura 6. Matriz para la identificación de los servicios críticos. 66

Figura 7. Análisis de impacto de negocios la identificación de los servicios crítico..... 67

Figura 8. Tipo de dependencia entre servicios la identificación de la ICC. 68

Figura 9. Modelo de Coordinación Nacional..... 70

Figura 10. Partes interesadas en la identificación de la ICC..... 72

Figura 11. Flujograma para la protección e identificación de las ICC. 75

Figura 12.Porcentaje de encuestados por sectores estratégicos de la ICCC. 77

Figura 13. Porcentaje de expertos que consideran necesaria la actualización de la Guía. 79

Figura 14. Porcentaje de expertos que piensan que los criterios deben ser modificados. 80

Figura 15. Porcentaje de encuestados por niveles de la ICC. 83

Figura 16. Porcentaje de experiencia de los encuestados en la administración de la ICC. 84

Figura 17. Conocimiento de la guía para la identificación de la ICCC. 85

Figura 18. Porcentaje de participación en la identificación de la ICCC. 86

Figura 19. Criterios de Criticidad para la identificación de la ICCC 88

Figura 20. Enfoques para el diseño de la Guía Metodológica para la identificación de ICCC.. .. 89

Figura 21. Criterios de criticidad para la identificación de las ICCC. 94

Figura 22. Escala de valoración impacto en los sectores estratégicos. 98

Figura 23: Actividades para la identificación de las Infraestructuras Criticas Cibernéticas de Colombia. 105

Lista de tablas.

Tabla 1. Riesgos de la Seguridad Digital. 39

Tabla 2. Número de sectores identificados en las Infraestructuras Críticas. 41

Tabla 3. Lineamientos, Políticas y Guías de las ICCC. 43

Tabla 4. Actividades para la identificación de la infraestructura critica cibernética. 52

Tabla 5. Definición de conceptos 55

Tabla 6. Relación de metodologías de identificación de ICC. 57

Tabla 7. Sectores estratégicos de Colombia. 72

Tabla 8.Porcentaje expertos por sectores estratégicos de la ICC 78

Tabla 9. Codificación del personal encuestado representantes de la ICCC. 81

Tabla 10. Porcentaje de participación en la identificación de la ICCC. 85

Tabla 11. Criterios de criticidad en la Guía metodológica para la identificación de la ICC. 88

Tabla 12. Listado de Criterios para la identificación de la ICC 92

Tabla 13. Escala de impacto en la salud pública y seguridad humana. 96

Tabla 14. Escala de Impacto económico 97

Tabla 15. Escala de Impacto en la Interdependencia de las Infraestructuras 99

Tabla 16. Escala de Impacto del tiempo de recuperación de la infraestructura. 100

Tabla 17. Escala impacto ambiental. 101

Tabla 18. Orden de relevancia de los criterios de acuerdo a la encuesta a expertos. 102

Tabla 19. Relevancia y peso de los criterios propuestos. 103

Tabla 20. Matriz de criterios para la identificación de las ICCC..... 103

Tabla 21. Principales sectores y subsectores críticos de Colombia. 106

Tabla 22. Sector, subsector y servicios esenciales..... 109

Tabla 23. Porcentajes para identificar operadores y empresas potencialmente catalogadas como críticos..... 110

Tabla 24. Lista de Actividades de la Guía Metodológica de ICCC..... 114

Introducción.

La sociedad depende de Infraestructuras Críticas (IC) con disponibilidad y funcionamiento adecuado que cubran las necesidades básicas de los habitantes de una nación. Es una de las prioridades de los Estados salvaguardar las instalaciones de mayor importancia para la población, cuya destrucción o interrupción podría generar serias consecuencias, tales como escasez de suministros y alimentos a largo plazo, corte de energía eléctrica, alteraciones de orden público y consecuencias en cascada a otras infraestructuras.

Las IC y ICC, son consideradas sistemas diferentes, cuando sus componentes y procesos son objeto de análisis. No todas las IC son consideradas ICC y pueden fallar por muchas razones no relacionadas con un componente cibernético; las fallas más comunes de las IC son la obsolescencia de su maquinaria y los desastres naturales como un terremoto o una inundación. Caso opuesto ocurre en una ICC, en donde a raíz de su conectividad, sus fallas son causadas esencialmente por ataques ciberneticos (Mahan, T & Menold, J, 2020). Sin embargo, dadas las condiciones del desarrollo tecnológico actual las dos infraestructuras, IC e ICC, no pueden ni deben considerarse como conceptos completamente separados. Por esta razón, durante el desarrollo de este trabajo, la ICC es considerada parte esencial y un subconjunto de una IC.

Las infraestructuras se ven amenazadas por los ataques terroristas o desastres naturales, como los ataques terroristas del 11 de septiembre de 2001 en la ciudad de Nueva York, los ocasionados en Madrid en el año 2004 y en Londres en 2005 o como el tsunami de Japón en el año 2011 que causó el colapso en una central nuclear; pero hay otro tipo de riesgos y amenazas que las sociedades deben enfrentar causadas por errores humanos, ingeniería social y vulnerabilidades en sus sistemas de información y redes de datos.

Un ejemplo de ello ocurrió en el año 2003, cuando las computadoras que alojaban el sistema de visualización de parámetros de seguridad de la planta de energía nuclear Davis-Besse en los Estados Unidos de América ocasionó consecuencias catastróficas cuando sus sistemas fueron infectados a través una técnica de inyección SQL (Miller, 2012). Otra serie de ejemplos, ocurrieron del año 2010 al 2012, cuando las variantes de un software malicioso, incluido el Stuxnet, Flame, Duqu y Gauss infectaron los controladores lógicos programables de los sistemas de control industrial de algunas plantas nucleares y provocaron daños físicos en los sistemas de información en varios países (Li, 2017).

Por otro lado, el 17 de noviembre de 2019, se notificó al mundo el primer caso de un nuevo coronavirus (COVID-19) en la ciudad de Wuhan (China), su transmisión de persona a persona se ha acelerado en todo el mundo, por lo que la Organización Mundial de la Salud la ha declarado una pandemia[1] a nivel mundial. Con esto, las Infraestructuras Críticas (IC) se han visto amenazadas a través de consecuencias biológicas.

Por ejemplo, el 6 de marzo de 2020, la Agencia de Seguridad de la Ciberseguridad e Infraestructura - CISA[2] de los EE. UU., lanzó una alerta sobre las posibles estafas relacionadas con la enfermedad del coronavirus (COVID-19), donde se han enviado masivos mensajes electrónicos con archivos adjuntos maliciosos o enlaces a sitios web fraudulentos para engañar a las víctimas para que revelen información confidencial y a través de acceso remoto instalar software malicioso en los sistemas de información y comunicaciones que operan las IC.

Los ejemplos anteriores permiten ilustrar que las Infraestructuras Críticas Cibernéticas (ICC) son una parte esencial de cualquier IC debido a que es considerada el eje principal para la

---

[1] Organización Mundial de la Salud (2020), consultada el día 23-MAR-2020. https://www.who.int/es/home

[2] CISA (Cyber-Infrastructure), consultada el día 23-MAR-2020. https://www.cisa.gov/identifying-critical

transferencia de información y las telecomunicaciones entre los sistemas que la componen. Las sociedades actuales dependen en gran medida de servicios vitales, como electricidad, transporte, transacciones financieras y tecnología de la información (TI). Es por esto, que en los países desarrollados consideran la identificación, catalogación y priorización de la ICC como un elemento esencial para formular estrategias, políticas, lineamientos y guías en pro de su protección y aseguramiento (Villalba, 2015), con el fin de evitar consecuencias catastróficas.

En América Latina, con los recientes cambios en su desarrollo que producen modernización y expansión de los servicios vitales para la sociedad, se han revelado nuevos y poderosos riesgos en los activos y sistemas de infraestructura; riesgos que se agravan con la dependencia generalizada y la creciente interconectividad de los diferentes servicios esenciales a nivel nacional. Esa interdependencia podría generar en las infraestructuras, interrupciones a gran escala y con efectos en cascada que afectarían directamente a la población (Garcia Zaballos, 2016).

Lo anterior permite comprender la importancia para Colombia de la actualización de la guía metodológica para la identificación de la ICC; dado que a la fecha no existe un listado de servicios críticos que se encuentren plenamente identificados, catalogados y priorizados se dificulta la protección en su totalidad de los activos esenciales para la seguridad y defensa nacional.

Es de especial importancia establecer la interdependencia entre los servicios vitales, teniendo en cuenta subsectores y sectores estratégicos, de tal modo que se logre proteger adecuadamente, evitando graves crisis socioeconómicas.

Capítulo I

Generalidades del trabajo de investigación.

En este capítulo se describe la importancia de la identificación, catalogación y priorización de la Infraestructura Crítica Cibernética de Colombia. Así como también, las consecuencias que ha ocasionado la ausencia de su aplicabilidad en las tecnologías de la información. También se relacionan los objetivos, alcance y metodología que se implementan en el desarrollo de esta monografía.

1.1 Descripción del problema.

Las Infraestructuras Críticas (IC) son aquellas instalaciones mediante las cuales se ofrecen servicios esenciales para la supervivencia de una sociedad, tales como: la distribución de agua, las telecomunicaciones, el transporte aéreo, marítimo y terrestre, la energía eléctrica, entre otras, estas infraestructuras han incrementado la interconexión entre ellas con el fin de transferir datos, compartir recursos y reducir esfuerzos (Mattioli, 2014).

Las IC pueden ser vistas desde tres perspectivas; la primera, la importancia simbólica para un país, ejemplo: museos, edificios y monumentos; la segunda, la dependencia directa con la energía eléctrica y las telecomunicaciones y la tercera la interconectividad con otras infraestructuras donde al fallar una de ellas podría causar el colapso de las otras (Rinaldi, 2004). Las Infraestructuras Críticas Cibernéticas (ICC) se puede definir como aquellas redes de computadoras, servicios, sistemas y tecnología de la información que, si se interrumpen o se alteran, tienen un grave impacto en la seguridad nacional y ocasionarían una pérdida económica para uno o varios sectores (Herrera L. C., 2019).

Un ciberataque tiene como objetivo explotar vulnerabilidades en los dispositivos electrónicos de un sistema, interconectado o no a Internet, generando no solo grandes consecuencias financieras, sino también la pérdida de vidas humanas (Frett, 2015). Sin embargo, en el momento de identificar, priorizar y proteger los servicios vitales de una sociedad, se debe tener en cuenta que no todos los sistemas interconectados pueden definirse como parte de la ICC de un país.

El creciente número de ciberataques contra la ICC ha convertido al ciberespacio en otro campo de batalla, donde las armas convencionales han sido reemplazas por dispositivos periféricos como el ratón y el teclado. Un ejemplo de ello, fueron los ataques cibernéticos ocurridos en Estonia en el 2007, cuando el gobierno anunció que movería la estatua "Soldado Ruso de Bronce" hacia las afueras de la ciudad de Tallin, lo que ocasionó disturbios sociales y una serie de ciberataques contra la disponibilidad, confidencialidad e integridad de los sistemas de información del Estado y el sector financiero (Pipyros, 2018).

Ucrania también fue anfitrión de un devastador ciberataque en diciembre de 2015, cuando 30 subestaciones del sistema nacional de energía eléctrica, fueron deshabilitados por más de 8 horas, afectando a una gran proporción de la población y otras infraestructuras, hospitales, servicios aéreos y ferroviarios (Liang, 2016).

Algunos países cuentan con herramientas particulares de acuerdo con las características propias de la nación para proteger los servicios y/u operadores que ellos han considerado como críticos (Herrera, 2019). Estados Unidos, Inglaterra, Francia y Alemania, han diseñado lineamientos, políticas, estrategias y guías para asegurar y proteger las ICC de atacantes internos, países enemigos y hacktivistas. En el caso de Francia, se ha implementado el enfoque Operator-based para identificar doce sectores y 220 operadores críticos de su país, mientras que Suiza

implementó el Service-Oriented para identificar 10 sectores y 28 servicios críticos.

En el caso de Colombia, se han venido realizando esfuerzos con el fin de generar estrategias que permitan ejercer una labor de ciberseguridad y ciberdefensa[3], una de ellas es el CONPES 3701, el cual tiene como objetivo central el fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, en dicho documento se señala como uno de los objetivos específicos, el implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y emergencias cibernéticas para proteger la infraestructura crítica nacional (DNP, 2011).

Siguiendo los lineamientos del documento CONPES mencionado se genera una estructura del estado colombiano conformada por: el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), el Comando Conjunto Cibernético de las Fuerzas Militares (CCOCI) y el Centro Cibernético Policial (CCP) para la asistencia, coordinación, desarrollo, gestión y asesoramiento en asuntos cibernéticos.

El CCOCI tiene como función principal prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales, es el encargado de direccionar y desarrollar, en concurso con diferentes organizaciones y entidades del Estado y del

---

[3] La Seguridad de las Tecnologías de Información y Comunicaciones (STIC) o "Ciberseguridad" tiene por objetivo la protección de los sistemas de información y comunicaciones y la información manejada por los mismos a través de la puesta en práctica de las medidas técnicas y organizativas apropiadas. Este tipo de medidas se enmarcan dentro de un marco más general denominado "Seguridad de la Información" que abarca desde la seguridad física y de personal, hasta STIC (Centro Criptológico Nacional, 2013), ahora bien, la ciberdefensa se define como: "La capacidad de asegurar y salvaguardar la prestación de los servicios, confidencialidad, integridad y disponibilidad, proporcionados por los Sistemas de Información y Comunicaciones en la fase de operación de los sistemas en producción, en respuesta a posibles inminentes acciones maliciosas originadas en el ciberespacio" (Fundación In-Nova Castilla La Mancha, 2019, Pág. 9)]

sector privado, la selección de las ICC. En el CCOCI se han desarrollado diferentes iniciativas que permiten anualmente emitir un catálogo de ICC de la nación, pero la guía para establecer dicho catálogo, solo cuenta con tres criterios que determinan la criticidad de los servicios vitales de la nación: daño al medio ambiente, perjuicios económicos y afectación a la población civil. Sin embargo, con estos tres elementos, el proceso de la identificación de las ICC, no permite determinar su verdadera criticidad, más aún si se tiene en cuenta la relevancia y riesgo de estas para la obtención de los objetivos nacionales, toda vez que criterios como la interdependencia y la gobernabilidad que son empleados a través de las metodologías o enfoques en otros países no son tenidos en cuenta en la guía actual.

Por lo anterior se requiere identificar los principales criterios que impactan a una infraestructura catalogada como crítica, haciendo uso de reformulación y aplicación de conceptos, lineamientos y políticas del orden nacional e internacional, que le permita al Estado colombiano a través del Comando Conjunto Cibernético, identificar, catalogar y priorizar las infraestructuras críticas cibernéticas, generando un inventario no muy amplio de infraestructuras, hacia las cuales se puedan direccionar los presupuestos, medidas de seguridad y protección respectiva, por parte de los diferentes actores encargados de la ciberseguridad y ciberdefensa de la nación, con el fin de garantizar el orden público de la nación. La no solución a este problema, aumenta la vulnerabilidad de los servicios esenciales, al no tener la claridad de la relevancia e importancia de las ICC que se deben proteger.

1.2 Justificación e impacto.

En la actualidad los Estados, sus organizaciones, empresas, compañías y la sociedad en general dependen de la provisión de servicios esenciales como electricidad, agua, transporte, comunicaciones, entre otros; servicios que a menudo necesitan estar interconectados entre sí y

bajo el control de TIC (Herrera L. C., 2019), lo que genera una dependencia del uso y empleo del ciberespacio por parte de las Infraestructuras Críticas y así mismo aumenta la probabilidad de interrupciones a estas, que podrían afectar el buen funcionamiento de un Estado y su sociedad.

La definición de ICC se refiere a la identificación y protección de sectores críticos, tales como energía, transporte, agua, alimentos, entre otros, pero cada país establece su ICC según políticas y estrategias nacionales de acuerdo con las necesidades y características particulares de la región.

Ejemplo de lo anterior es el caso de la Unión Europea no todos sus países han aplicado una herramienta encaminada a proteger las ICC; por tal razón, el 8 de agosto de 2016 entró en vigencia la Directiva 1148 del Parlamento Europeo, a partir de ese momento, los Estados miembros cuentan con 21 meses para transponer dicha directiva a sus leyes nacionales y otros seis meses para identificar al menos los operadores de servicios esenciales (Diario Oficial de la Unión Europea , 2016).

Por otro lado, en Latinoamérica, la estandarización y esfuerzos de la Organización de los Estados Americanos (OEA) para la identificación y protección de las ICC han permitido la priorización y asignación de recursos en los diferentes países con el fin de evitar interrupciones generadas por los ciberataques en sus servicios críticos (Organization of American States, 2018); sin embargo, al igual que en la Unión Europea, los Estados miembros de la OEA no aplican los mismos enfoques, herramientas, políticas y estrategias debido a factores particulares, como: la cultura, la geografía, los hábitos, los riesgos, la religión, las prioridades y las responsabilidades, entre otras. Así es que, por ejemplo, Chile cuenta con una política nacional de ciberseguridad 2017-2022 dedicada a la identificación, jerarquización y protección de las infraestructuras críticas de la información (Gobierno de Chile, 2017).

Durante los últimos años la comunidad internacional ha realizado diferentes investigaciones relacionadas a la identificación y metodologías de análisis de las Infraestructuras Críticas, un insumo base para la elaboración de planes de resiliencia, para el desarrollo de políticas de Estado y planes de protección a infraestructuras críticas. (Gómez, 2018).

Es así como diferentes países de la Unión Europea y el continente americano han llevado a cabo actividades para definir la metodología a través de la cual logren la identificación de su Infraestructura Critica Cibernética Nacional (ICCN), teniendo en cuenta que se requiere que los métodos sean muy precisos y de esta manera determinar bien lo que debe ser protegido.

Colombia ha realizado esfuerzos significativos para la identificación de las ICC, con la primera edición de la Guía para la Identificación de la Infraestructura Crítica Cibernética del año 2015 y la generación de documentos CONPES 3701 y 3854 con políticas para mejorar el fortalecimiento de la capacidad de cada Estado frente a amenazas que atentan contra la seguridad y defensa en el ámbito cibernético.

El panorama actual en Colombia en cuanto a masificación del uso de las TIC y ampliación de su espectro en el ciberespacio lo registro así la revista Dinero (2018): "Mientras que el 44% de los latinoamericanos no tiene acceso a la red, en Colombia la introducción del internet llegó al 61,4% de la población". Dentro de esta cobertura se encuentran incluidos todos los campos de acción del Estado (económico, político, social y militar); es en esos campos donde se encuentran las infraestructuras críticas, es decir, cuyo daño puede aparejar consecuencias negativas sobre la seguridad de las personas y la seguridad estatal (Rodriguez, 2019), por cuanto su ataque, interrupción o destrucción afectarían la salud, la seguridad o el bienestar económico de los ciudadanos.

Dicha posibilidad de afectación genera obligaciones para el estado colombiano, en cuanto a contar y fortalecer las capacidades de ciberdefensa y ciberseguridad que permitan la protección de la infraestructura crítica; una manera de lograrlo ha sido generando políticas y modelos en seguridad y defensa; pero es necesario el análisis de diferentes marcos de referencia y de modelos que permiten entender cómo Colombia selecciona su Infraestructura Crítica Cibernética.

Este análisis del proceso de identificación de ICC contribuye a determinar los puntos débiles para posibles ataques de impacto nacional; ya que identificados correctamente los servicios y operadores vitales para el país se puede llevar a cabo de una manera más precisa el inventario y su priorización, en búsqueda de la protección de riesgos comunes y/o externos que se pueden presentar en el ir y venir de las actividades nacionales; de esta manera se mitigan las amenazas que enfrentan los servicios esenciales y así mismo, se cuenta con información técnica para generar políticas de salvaguarda y defensa nacional.

Cabe resaltar ademas, que fue realizada una encuesta a personal de expertos en ICC, quienes poseen conocimiento y experiencia en temas administrativos, operativos y académicos relacionados con las ICC, pertenecientes a los diferentes sectores estratégicos del Estado colombiano, quienes participan en las reuniones de "Infraestructura Critica, Riesgo Operacional y Ciberdefensa", con el fin de determinar la necesidad de la actualización de la guía actual y justificar su desarrollo.

Mediante los resultados obtenidos, se logra establecer que el 75% de los encuestados consideran la necesidad de modificar los criterios actuales y un 25% consideran que no es necesario. Este resultado nos indica que es ineludible el trazado de ajustes o nuevos criterios, situación ante la cual se justifica el trabajo de investigación, buscando generar un impacto a nivel

nacional teniendo en cuenta que se afectaran a las Infraestructuras Criticas Cibernéticas de Colombia.

1.3 Pregunta de Investigación.

¿Cómo mejorar la identificación de las Infraestructuras Críticas Cibernéticas (ICC) de Colombia?

1.4 Alcance.

El alcance de esta investigación se enmarca en el análisis comparativo y conceptual de marcos de referencia, modelos y metodologías existentes, así como el análisis de fuentes de datos primarios recolectados a expertos y operadores de Infraestructura Crítica en Colombia, que permita generar una propuesta para actualizar la guía existente de identificación de ICC Colombiana (ICCC) diseñada por el Comando Conjunto Cibernético en el año 2015.

1.5 Objetivo Principal.

Proponer nuevos criterios que permitan actualizar la guía metodológica para la identificación de la Infraestructura Crítica Cibernética de Colombia.

1.6 Objetivos Específicos.

a) Analizar metodologías, lineamientos e información académica que permita establecer las mejores prácticas en el proceso de identificación de las Infraestructuras Críticas Cibernéticas.
b) Aplicar un método de recolección de datos primarios para identificar las características, criterios o variables de las Infraestructuras Críticas Cibernéticas.

c) Establecer el proceso para la nueva guía metodológica para la identificación de la Infraestructuras Críticas Cibernéticas de Colombia del Comando Conjunto Cibernético.

1.7 Metodología.

En este trabajo la metodología de investigación es pragmática, por cuanto investigar es crear conocimiento para resolver problemas prácticos (Hurtado, 2012). El tipo de investigación es investigación prospectiva, la cual usa el análisis de información para diseñar o crear propuestas dirigidas a resolver determinadas situaciones. Se combinarán técnicas cualitativas y cuantitativas. En cuanto a la información cualitativa se aportará descripción comparativa de diferentes metodologías o enfoques llevados a cabo por otros países para la identificación de las ICC, y los datos cuantitativos se generan en la tabulación de información de diferentes expertos en ICC.

El presente trabajo se considera monografia, teniendo en cuenta lo afirmado por Hurtado (2012) "la documentación dirigida a organizar conocimiento existente son las monografías" (p 39). El proceso para el desarrollo de la presente monografía será abordado a través de las siguientes fases:

a) Analítica: en esta fase se obtuvieron las fuentes documentales disponibles sobre los conceptos relacionados con las ICC; igualmente se registran métodos o enfoques empleados en diferentes países u organizaciones, lo cual permita obtener información de manera integral y holística.

b) Comparativa: en esta fase se revisaron antecedentes de investigaciones previas y se compararon los enfoques de identificación de ICC existentes, lo que permitió captar

lo común y lo diferente entre ellas para determinar las buenas prácticas en el proceso de identificación.

c) Interactiva: en esta fase se hizo la recolección de datos a través de encuestas, realizadas a personal de expertos en ICC, que nos permita establecer y determinar elementos de valor para el desarrollo de la monografía.

d) Confirmatoria: en esta se hizo el análisis de los datos obtenidos, con la intención de darle un significado, que nos permita el cumplimiento del objetivo planteado.

La recolección de información estará basada en: (a) análisis de documentos oficiales de fuentes primarias generadas por el MINTIC y el CCOCI, e información de fuentes secundarias, como: lineamientos, políticas, estrategias, guías e información académica aplicables a la propuesta; (b) herramienta de recolección de información aplicada a los operadores de las Infraestructuras Criticas del País y expertos académicos en ciberseguridad; y, (c) diseño del proceso para establecer una guía metodológica para la identificación de la ICCC.

A continuación, en primer lugar se registra el análisis conceptual de las teorías, estándares y metodologías existentes para la identificación, priorización y catalogación de las Infraestructuras Críticas Cibernéticas (ICC); luego se efectuara la recolección de datos primarios por intermedio de dos encuestas, para identificar la necesidad de la modificación de la guía metodológica actual, al igual que la pertinencia de nuevos criterios para el proceso de Identificación de las Infraestructuras Críticas Cibernéticas en Colombia (ICCC), entre otros elementos, que permitan entender la visión y aprovechar la experiencia de expertos en la protección de las ICCC. Por último, se sugiere el proceso de la nueva guía metodológica para la identificación de la Infraestructuras Críticas Cibernéticas de Colombia, a través de la propuesta de nuevos criterios que permitan una mejor priorización.

Conviene subrayar, que las encuestas realizadas no buscan hacer inferencias poblacionales, ni busca generar acuerdos para todo el modelo a través del cual se realice el proceso de identificación de las ICC, lo que se pretende es hacer un sondeo que permita emitir unas líneas de trabajo para efectuar la propuesta que a futuro conlleve a la actualización de la Guía Metodológica para la Identificación de las Infraestructuras Criticas Cibernéticas de Colombia.

Capítulo II

Infraestructura crítica e infraestructura critica cibernética.

En la presente sección se expone el contexto de la investigación estableciendo la diferencia entre las Infraestructuras críticas e Infraestructuras Criticas Cibernéticas, teniendo en cuenta que no todas las IC son ICC, lo que hace pertinente dejar claridad de esta diferencia, al igual que se pretende dar a conocer los sectores en los cuales se agrupan esos servicios esenciales que suministran las IC y la necesidad de su protección.

2.1 Conceptos básicos.

Para lograr lo anterior es necesario comprender los siguientes conceptos:

a) Ciberespacio: Es el ambiente, tanto físico como virtual, compuesto por sistemas computacionales, programas y aplicaciones (software), redes de telecomunicaciones incluido el internet, datos e información y la infraestructura física asociada que es utilizada para la interacción entre usuarios, entre máquinas y entre máquinas y usuarios (CCOCI, 2016).

b) Ciberseguridad: La ciberseguridad debe entenderse como la protección de los intereses vitales de la persona y el ciudadano, la sociedad y el Estado al utilizar el ciberespacio. (Vakulyk, O., & Petrenko, P., 2020).

c) Ciberdefensa: La ciberdefensa se ocupa de la protección de la información en la búsqueda de la lucha contra ataques que vulneren la soberanía y control de los recursos tecnológicos e informáticos (Valencia, A., Patiño, O., & Garces, L., 2020).

d) Ciberataque: Un ciberataque es cuando alguien obtiene o intenta obtener acceso no autorizado a un sistema informático de forma maliciosa con la intención de dañar o alterar los sistemas o robar información valiosa de dicho sistema (Teymourlouei, 2015).

e) Tecnología de Información (IT): La tecnología que involucra el desarrollo, mantenimiento y uso de computadoras, sistemas, software y redes para el procesamiento y distribución de datos (Hahn, 2016).

f) Tecnología Operacional (OT): El equipamiento, dispositivos, sensores y software utilizados para controlar o monitorear activos físicos y procesamiento en tiempo real con el propósito de mantener la integridad del sistema (Gartner, 2015).

g) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y las administraciones públicas (CCOCI, 2016).

h) Ingeniería Social: es una técnica basada en el engaño y busca manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas, para sacar provecho de las debilidades de una persona. Estas contemplan: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (Méndez, 2018).

i) Guía metodológica: una guía metodológica es la sistematización y documentación de un proceso, actividad, práctica, metodología o proceso de negocio. La guía describe las distintas operaciones o pasos en su secuencia lógica, señalando generalmente quién, cómo, dónde, cuándo y para qué han de realizarse (Robles, 2017).

2.2 Conceptos relacionados con la Infraestructura Crítica.

Las sociedades han enfrentado y vienen enfrentando riesgos y amenazas que afectan sus infraestructuras críticas (IC), como los ataques terroristas del 11 de septiembre de 2001 en la ciudad de Nueva York, los ocasionados en Madrid en el año 2004 y en Londres en 2005, los

desastres naturales, eventos como la erupción del volcán Eyjafjallajökull (2010), el terremoto y tsunami de Tōhoku (2011) y el huracán Sandy (2013), sumado a estos los errores humanos, la ingeniería social, y vulnerabilidades en los sistemas de información y redes de datos; son riesgos y amenazas que generan amplios efectos en una sociedad globalmente conectada en red (Pescaroli & Alexander, 2016).

Infraestructura se refiere a "el conjunto de elementos, dotaciones o servicios necesarios para el buen funcionamiento de un país, de una ciudad o de una organización cualquiera" (Real Academia de la Lengua Española, 2020). Desde hace décadas las sociedades cada día cuentan y desean contar con más elementos o servicios con el fin de satisfacer sus necesidades vitales, situación que conlleva a la realización de esfuerzos cada vez más complejos por parte de los Estados.

Dentro de todos los servicios a los que se refiere la definición existe un conjunto de infraestructuras que dan soporte y facilitan el normal funcionamiento de los sectores productivos, de gestión y de la vida ciudadana en general, las cuales se consideran críticas para la sociedad; son críticas porque su inoperatividad, afectación o interrupción puede alterar a otros sistemas que pueden generar grandes efectos.

Aunque no existe una única definición, cada país u organización define sus Infraestructuras Críticas (IC) de acuerdo con sus necesidades. Un ejemplo de esto son las definiciones que se referencian a continuación:

Colombia las define como "las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales" en documento elaborado desde el Comando Conjunto Cibernético (CCOCI, 2016).

Estados Unidos las define como "los activos, sistemas y redes, ya sean físicos o virtuales, tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante sobre la seguridad, la seguridad económica nacional, salud pública o seguridad nacional, o cualquier combinación de estas" (USA, 2001).

La Unión Europea, a través de la directiva 2008/114/CE, las define como "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones".

La North Atlantic Treaty Organization (NATO) también ofrece una definición de infraestructuras críticas en su documento Critical Infrastructure Protection against Terrorist Attacks, publicado en noviembre de 2014 "como aquellas instalaciones, servicios y sistemas de información que son tan vitales para las naciones que su incapacidad o destrucción tendría un impacto debilitador en la seguridad nacional, la economía nacional, la salud pública y la seguridad y las funciones efectivas de un gobierno" (NATO, 2014).

Desde una perspectiva más global, las IC son aquellas instalaciones mediante las cuales se ofrecen servicios esenciales para la supervivencia de una sociedad, tales como: la distribución de agua, las telecomunicaciones, el transporte aéreo, marítimo y terrestre, la energía eléctrica, entre otros; estas infraestructuras han incrementado la interconexión entre ellas con el fin de transferir datos, compartir recursos y reducir esfuerzos (Mattioli, 2014).

Las IC pueden ser vistas desde tres perspectivas: (a) La importancia simbólica para un país, ejemplo: museos, edificios y monumentos; (b) La dependencia directa con la energía eléctrica y las telecomunicaciones; y, (c) La interconectividad con otras infraestructuras donde

una falla en una de ellas podría causar el colapso de las otras (Tabansky, 2011).

Según (Rinaldi, 2004), la interconexión de la IC se analiza desde cuatro perspectivas:

a) A través de una interdependencia geográfica: cuando dos o más infraestructuras comparten una proximidad espacial.
b) Cuando existe una interdependencia lógica: dos o más infraestructuras son lógicamente interdependientes si el estado de una infraestructura depende del Estado y/o disponibilidad de otra infraestructura.
c) Mediante una interdependencia física: dos o más infraestructuras son físicamente interdependientes si un producto producido por una infraestructura es estrictamente necesario por otra infraestructura para que esta funcione correctamente.
d) A través de una interdependencia cibernética: cuya actividad principal se basa en el funcionamiento adecuado de las redes de información y comunicación

Las Infraestructuras Críticas (IC) también se analizan desde el punto de vista de la prioridad debido a disponibilidad y funcionamiento adecuado para cubrir las necesidades básicas de una Nación; es decir, el Estado tiene la obligación de salvaguardar en primer lugar las instalaciones de mayor importancia para la población, cuya destrucción o interrupción podría generar serias consecuencias, como escasez de suministros y alimentos a largo plazo, corte de energía eléctrica, alteraciones de orden público y consecuencias en cascada a otras infraestructuras.

Como resultado del análisis de los conceptos de infraestructuras críticas, se concluye que todos están direccionados hacia la importancia de protección de los servicios esenciales; pero el concepto planteado por la Unión Europea en la directiva 2008/114/CE de diciembre de 2008, se considera en este estudio el concepto más apropiado al integrar de manera holística los elementos

que definen la funcionalidad de un Estado y que al fallar ponen en riesgo su integridad.

2.3 Conceptos relacionados con la Infraestructura Crítica Cibernética.

Las infraestructuras críticas, a raíz del avance tecnológico, emplean sistemas de información y comunicación como medio para automatizar y optimizar muchas de las actividades que en ellas se realizan, permitiendo de esta manera que el manejo de información tome relevancia e importancia, convirtiendo a una IC en una Infraestructura Critica Cibernética (ICC), las cuales son consideradas el eje principal para para procesar, transferir, almacenar e intercambiar información (Christensen S., Caelli, W., Duncan W., & Georgiades, E,. 2010), con el fin de garantizar el funcionamiento, continuidad y disponibilidad de sus servicios.

Entonces, las infraestructuras criticas cibernéticas son redes de computadoras, servicios, sistemas y tecnología de la información que, si se interrumpen o se alteran, tienen un grave impacto en la seguridad nacional y ocasionarían una pérdida económica para uno o varios sectores (Hruza, 2018). Aunque similar a la definición aportada por Hruza, la definición de Estonia "sistemas de información y comunicaciones cuyo mantenimiento, fiabilidad y seguridad son esenciales para el buen funcionamiento de un país. La infraestructura de información crítica es parte de la infraestructura crítica"[4] permite precisar tres elementos: mantenimiento, fiabilidad y seguridad.

En Colombia fueron definidas las ICC como: "las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o tecnologías de la operación (OT), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave

---

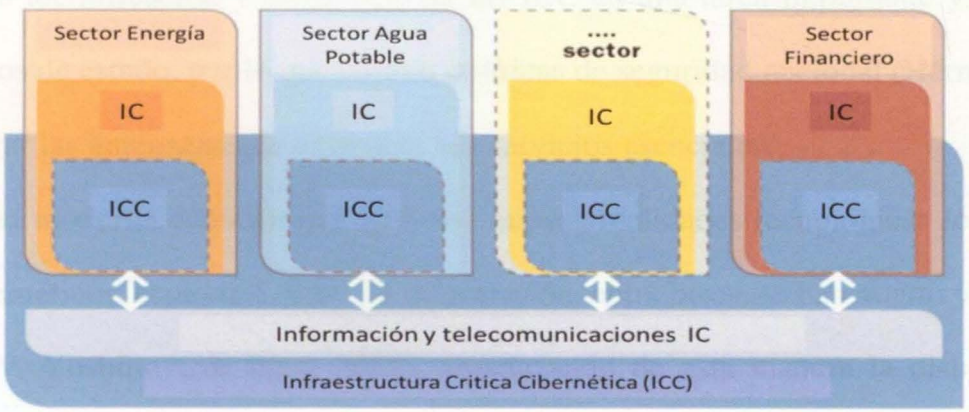
[4] Republic of Estonia, Information System Authority, Cybersecurity, Critical Information Infrastructure Protection. https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

impacto sobre los servicios esenciales" (CCOCI, 2016, p. 2). El término Infraestructuras Estratégica fue tomado de la ley 8/2011 del gobierno de España y se refiere a "las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales" (CCOCI, 2016, p. 2)

Así mismo, en el 2008 la OCDE a través del informe del concejo de las ICC, consideró que las ICC incluyen normalmente tres elementos: componentes de información que apoyan las IC y/o infraestructuras de información que apoyan a componentes esenciales de la gestión gubernamental y/o infraestructuras de información esenciales para la economía nacional. (OECD, 2008).

En consecuencia, la vulnerabilidad de la ICC tiene un efecto significativo y hasta total en el funcionamiento de una infraestructura crítica (Harasta, 2018) a raíz de la interdependencia informativa que se generan entre diferentes infraestructuras, como lo evidenciamos en la figura 1.

Figura 1. Interdependencia entre los sectores.



Fuente: Foro mundial sobre experiencia cibernética, (2017).

Estas interdependencias demuestran que la interrupción, perturbación y/o destrucción de una IC tendría consecuencias catastróficas con impacto intersectorial e incluso internacional; todo a raíz de la convergencia que se presenta entre la IT y la OT, las cuales se encuentran interconectadas a través de redes de datos y de procesos digitales, generando un control automático, utilizado tanto en los procesos industriales como en la gestión de las infraestructuras.

Ahora bien, el control automático de procesos es una de las disciplinas que se ha desarrollado a una velocidad vertiginosa en los últimos años y es indiscutible el reconocimiento universal de sus ventajas y beneficios asociados al ámbito industrial, de hecho, hoy en día es una actividad multidisciplinar, en la que hay que tener en cuenta aspectos técnicos (implicación de TIC), científicos (investigación de nuevos criterios y materiales, entre otros) y económicos (Stouffer, Falco & Scarfone, 2011).

Dicho de otra manera, los avances en tecnología digital han ocasionado la transformación en la forma en que las personas, las organizaciones y los Estados interactúan, dado que se emplea el ciberespacio como medio para su interacción, permitiendo el ingreso de nuevas amenazas; lo cual convierte a la identificación y protección de las ICC en una tarea importante y desafiante para los organismos de estado, por lo que emiten políticas de seguridad nacional (Herrera, 2019), con el fin de mitigar las amenazas que enfrentan sus servicios esenciales.

La sociedad moderna constata que ante sus nuevas realidades tecnológicas los términos como ataques cibernéticos, espionaje, robo de información, entre otros, se han vuelto y serán más comunes (Tsochev, Yoshinov, & Iliev, 2019), amenazando de esta manera la disponibilidad, confidencialidad e integridad de los sistemas de información, situación que puede conllevar a una interrupción, perturbación y/o destrucción de una ICC con consecuencias devastadoras y con impacto intersectorial.

Para concluir, los conceptos IC e ICC, no pueden considerarse conceptos separados a partir de la evidencia de una dependencia de la sociedad de la infraestructura altamente tecnológica e igualmente una creciente interconexión entre las infraestructuras. La ICC es una parte esencial y un subconjunto de una IC, este aspecto, unido a las referencias teóricas mencionadas ratifica que el concepto de ICC emitido por el CCOCI contiene los aspectos necesarios para el desarrollo del presente trabajo.

Tanto nuestro Estado colombiano como cualquier operador de ICC, requieren investigación que permita mejorar la seguridad de las redes de comunicación y los sistemas de información que soportan los servicios esenciales; por tanto, es esencial la identificación, catalogación y priorización de las ICCC.

2.4 Sectores de las Infraestructuras Críticas Cibernéticas y su protección.

En la actualidad la sociedad depende en gran medida de servicios esenciales, como: la electricidad, el transporte, las transacciones financieras y la tecnología de la información (IT). Es por esto, que en los países desarrollados consideran la identificación, catalogación y priorización de la ICC como un elemento esencial para formular estrategias, políticas, lineamientos y guías en pro de su protección y aseguramiento (Villalba, 2015).

El creciente número de ciberataques contra la ICC ha convertido al ciberespacio en otro dominio de la guerra, donde las armas convencionales han sido reemplazas por dispositivos periféricos como un mouse y un teclado.

Un referente común para señalar la importancia de la protección de las ICC es la experiencia de consecuencias catastróficas que generó el software malicioso "BlackEnergy" cuando infectó la red eléctrica de Ucrania y generó modificaciones para interrumpir los sistemas de control industrial. Esta fue la primera instancia conocida en la que un ciberataque provocó un

apagón a nivel nacional en su sistema eléctrico y donde los hackers obtuvieron acceso a los sistemas de control a través de una puerta trasera mediante el protocolo "Secure Shell" SSH; este ataque ocurrió el 23 de diciembre de 2015 durante aproximadamente ocho horas más de 225 mil usuarios quedaron sin servicio de electricidad, debido a que siete subestaciones de 110 kV de alta tensión y 23 subestaciones de 35 kV fueron desconectadas (Sans, 2016). Ningún operador y/o proveedor de IC aceptó públicamente, en la crisis, que habían tenido una interrupción por causa de un ciberataque, ataque que no solamente había sido planeado y coordinado previamente, sino que también tenía como objetivo dejar sin electricidad a todo un país por muchas horas, afectando a una gran proporción de la población y otras infraestructuras, como: hospitales, servicios aéreos y ferroviarios. (Liang, 2016)

Otro ejemplo de ataques cibernéticos de graves consecuencias es los ataques cibernéticos ocurridos en Estonia en el 2007; cuando el gobierno anunció que movería la estatua del "Soldado Ruso de Bronce" hacia las afueras de la ciudad de Tallin. Lo que ocasionó disturbios sociales y una serie de ciberataques contra la disponibilidad, confidencialidad e integridad de los sistemas de información del Estado y del sector financiero (Pipyros, 2018).

De acuerdo con lo publicado en el documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España, los principales riesgos cibernéticos a los que se exponen todos los usuarios del ciberespacio se pueden clasificar de la manera que se ilustra en la Tabla 1.

Los diferentes riesgos cibernéticos que se evidencian han generado el desarrollo de algunos conceptos para la protección ICC que se adaptan a las necesidades, características y prioridades de cada país. En el caso de la Unión Europea la definición destaca garantizar la funcionalidad, continuidad e integridad de las infraestructuras críticas, con actividades de

prevención, mitigación y neutralización tanto de amenazas como de riesgos o vulnerabilidades. Es así, como algunos Estados han diseñado estrategias, planes, lineamientos, guías y políticas precisas para identificar y proteger estos activos de ataques cibernéticos e interrupciones inesperadas (Herrera, 2019).

Tabla 1. Riesgos de la Seguridad Digital.

Riesgo Cibernético	**Descripción**
Fraude Financiero	Las instituciones y entidades financieras son uno de los principales objetivos de los ciberdelincuentes. El robo económico representa una de las principales motivaciones de la gran mayoría de ciberatacantes.
Robo de información	La información de carácter personal o documentos clasificados son algunos de los principales activos de información que deben ser especialmente protegidos. La filtración pública o pérdida de la información confidencial es un riesgo elevado, cuyos impactos o pérdidas pueden resultar especialmente significativos.
Indisponibilidad de servicios	Es la interrupción puntual o prolongada de los servicios ofrecidos en línea como por ejemplo correos, pagos financieros, cobro de impuestos, registros públicos, entre otros.
Sabotaje de infraestructuras	Son los ataques contra los servicios o infraestructuras críticas de un país o estado, provocando desabastecimientos, o interrupciones de comunicaciones, etc. con el objetivo de

Riesgo Cibernético	Descripción
	provocar una paralización puntual o prolongada de los mismos.
Pérdida de reputación	Es una de las principales consecuencias de las agresiones cibernéticas y el objetivo de gran parte de los ciberataques, cuyos efectos pueden resultar altamente significativos.

Fuente: Instituto de Auditores Internos de España, (2016).

En consecuencia, la identificación y protección de las ICC es una tarea importante y desafiante para los organismos de Estado, quienes emiten políticas de seguridad nacional. La necesidad de identificación de las ICC está motivada por preocupaciones de seguridad nacional, reducción de tiempo en el desarrollo de los procesos y consideraciones financieras (Herrera, 2019). Estos tres aspectos permiten resaltar la importancia de mejorar la seguridad de las redes de comunicación y los sistemas de información que soportan los servicios esenciales.

Por otra parte, las infraestructuras críticas existentes en un Estado se agrupan dentro de sectores estratégicos, aquellos que son esenciales para la seguridad nacional o para el conjunto de la economía de un país, como por ejemplo defensa, energía, transporte, salud, financiero, educación (CCI, 2013). En el año 2014, La Agencia Europea de Seguridad de las Redes y de la Información (ENISA por sus siglas en inglés) emitió una metodología donde se proporcionó una lista de once sectores potenciales, los cuales podrían ser identificados a través de dos enfoques: un enfoque dependiente del servicio no crítico y un enfoque dependiente del servicio crítico (Mattioli, 2014). Similar a esto, los Estados Unidos de América a través del Homeland Security, ha identificado y catalogado a 16 sectores como críticos para el País.

Colombia también a través de la cartilla "Sectores Estratégicos de la República de Colombia desde la óptica Cibernética" emitida por el CCOCI en el año 2016, establece que Colombia cuenta con 13 sectores estratégicos, sobre los cuales se lleva a cabo el proceso de identificación de las ICC.

Cada país lleva a cabo su selección de acuerdo a sus prioridades nacionales, a su características y reglamentación existente (ENISA, 2014). En la tabla 2, se relaciona la lista de algunos países y sectores esenciales identificados.

Tabla 2. Número de sectores identificados en las Infraestructuras Críticas.

Sector / País	**Colombia**	**Estados Unidos**	**Unión Europea**	**Francia**	**Alemania**	**Republica Checa**	**Chile**
Alimentación	X	X	X	X	X	X	
Agua	X	X	X	X		X	X
Comercio, Industria, Turismo	X			X			
Defensa	X	X		X			X
Educación	X						
Electricidad	X	X	X	X		X	X
Financiero	X	X	X	X	X	X	X
Gobierno	X	X		X	X	X	X
Recursos Naturales Medio Ambiente	X				X		
Recursos minero-energéticos	X						
Salud y protección social	X	X	X	X	X	X	X
Tecnologías de la información	X	X	X	X	X	X	X

Sector / País	Colombia	Estados Unidos	Unión Europea	Francia	Alemania	Republica Checa	Chile
Transporte.	X		X	X	X	X	X
Químico		X	X				
Instalaciones comerciales		X					
Medios y cultura							
Servicios de emergencia		X				X	
Manufacturas y fabrica		X					
Reactores nucleares, materiales y residuos		X	X				
Represas		X					
Espacio e investigación			XX	X			X
Seguridad publica							X
Protección civil							X
Actividades legales				X			
Total	**13**	**16**	**11**	**12**	**9**	**9**	**11**

Fuente: Elaboración propia a partir de las directrices para la protección de IC de los países relacionados y ENISA, (2020).

Igualmente, países como Inglaterra, Francia, Alemania, entre otros, han diseñado lineamientos, políticas, estrategias y guías para asegurar y proteger las ICC de atacantes internos, países enemigos y hacktivistas. En el caso de Francia, se ha implementado el enfoque "Operator-based" para identificar 12 sectores y 220 operadores críticos de su país, mientras que Suiza implementó el "Service-Oriented" para identificar 10 sectores y 28 servicios críticos. Estas metodologías han demostrado que los países cuentan con herramientas particulares de acuerdo

con las características propias de la nación para proteger los servicios y/u operadores que ellos han considerado como críticos (Mattioli, 2014).

Cabe resaltar, que en Colombia también se han realizado diferentes esfuerzos significativos para la protección de las ICC, en donde diferentes organismos y sectores han publicado lineamientos y políticas encaminadas a la protección de los activos críticos, como se muestra en la Tabla 3.

Tabla 3. Lineamientos, Políticas y Guías de las ICCC.

Sector	Producto	Objetivo	Resumen
MINTIC	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (2014-2015-2016)	Tener un enfoque estructurado y bien planificada que permita manejar adecuadamente los incidentes de seguridad de la información.	Lineamientos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información en Colombia.
MINTIC	Manual de Gobierno Digital (2018)	Mejorar y automatizar la gestión pública y la relación del Estado con los ciudadanos.	Lineamientos para el desarrollo de procesos de transformación digital al interior del Estado.
MINTIC	Guía de gestión de riesgos (2010-2016)	Gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad).	Resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida.
MDN	Guía para la identificación de infraestructura crítica cibernética de Colombia (2015).	Definir las actividades para la identificación de la infraestructura crítica cibernética del país.	Generar un listado de servicios esenciales y sectores estratégicos del país.

Sector	Producto	Objetivo	Resumen
DNP	CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa (2011)	Generar lineamientos de política en ciberseguridad y ciberdefensa.	Lineamientos orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan al País.
DNP	CONPES 3854. Política Nacional de Seguridad Digital (2016)	Fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital	Asignar recursos financieros y crear las instancias de coordinación y orientación superior en torno a la seguridad digital en el gobierno.

Fuente: Elaboración propia a partir de la regulación colombiana existente, (2020).

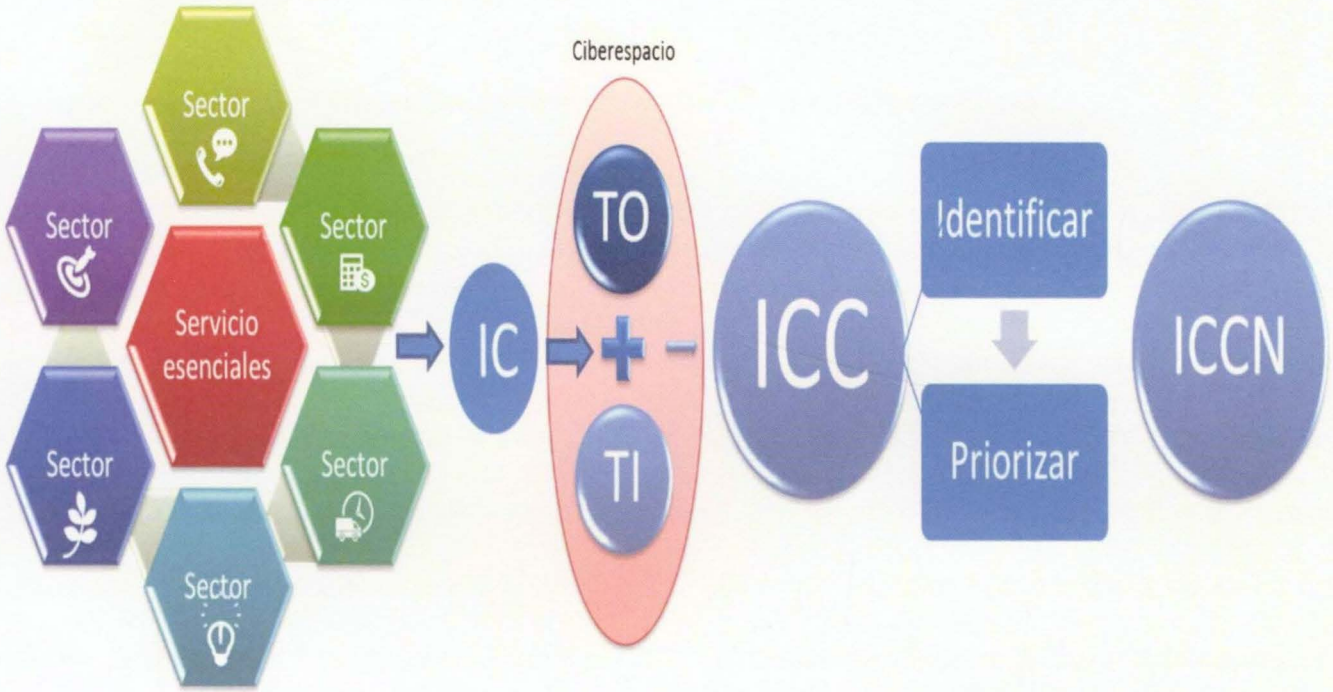
Aunque todas las Infraestructuras son importantes se requiere una buena identificación, con el fin de determinar sobre cuáles se debe enfocar una mayor atención, tanto en situaciones normales como en emergencia; teniendo en cuenta el impacto de su interrupción en la vida de las personas, la economía del país, la seguridad de los ciudadanos, entre otras.

Para los sectores de Infraestructuras Criticas Cibernéticas, un ciberataque tiene como objetivo explotar las vulnerabilidades en los dispositivos electrónicos de un sistema interconectado o no, a través del ciberespacio, generando grandes consecuencias económicas, la pérdida de vidas humanas y de la gobernabilidad. Estas situaciones obligan a identificar aquellas Infraestructuras que requieren de una mayor protección en los sectores estratégicos categorizados por cada Estado, como lo vimos en la Tabla 2; sectores en donde se concentran los servicios

esenciales para el buen funcionamiento del Estado, los cuales presentan una dependencia en las TIC, como se representa en la Figura 2.

Los sistemas de comunicación no se consideran críticos en sí mismos, su criticidad se basa en su control directo o influencia sobre otro activo de infraestructura crítica. Sin embargo, en el momento de identificar, priorizar y proteger los servicios esenciales de una sociedad, se debe tener en cuenta que no todos los sistemas interconectados pueden definirse como parte de la ICC de un país.

Figura 2. Las Infraestructuras Criticas Cibernéticas.



Fuente: Elaboración propia, (2020).

Así mismo, conviene subrayar, en el año 2015, ante la necesidad de la protección de las ICC, Colombia publicó la Guía Metodológica para la identificación de ICC de Colombia, con el propósito de:

> "Definir las actividades para la identificación de la infraestructura crítica cibernética del país, en el marco del manejo de riesgo operacional, Ciberseguridad y Ciberdefensa liderada por el Comando Conjunto Cibernético (CCOC) en coordinación con el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional" (CCOCI 2016, p.3).

Capítulo III

Mejores prácticas en el proceso de identificación de las ICC.

A continuación, se presenta un análisis de la actual Guía Metodológica para la Identificación de las ICC de Colombia; se relacionan los entes y organismos públicos y privados que están involucrados en el proceso de identificación de las Infraestructuras Críticas Cibernéticas en Colombia y se expone el análisis de las mejores prácticas para el proceso de la identificación de las ICC. Así mismo se presentan elementos útiles para la actualización de la Guía Metodológica para identificación de las ICC, tomados de la información recolectada de las políticas y metodologías ya existentes en el mundo.

3.1 Criterios para determinar las infraestructuras Críticas Cibernéticas.

El flujo de información ejerce el control en una sociedad cada vez más globalizada, al igual que la tecnificación de bienes y servicios, que ahora funcionan por medio de computadoras a través del nuevo dominio de la guerra, el ciberespacio. Las TIC están integradas en diferentes aspectos de la vida diaria, desde la capacidad de comunicarse con otras personas alrededor de mundo, hasta la de permitir que infraestructuras puedan proporcionar sus servicios como electricidad y telefonía al Estado y a la sociedad, al igual que articular la seguridad nacional y las redes de defensa; por lo tanto, una interrupción de TIC con funciones críticas puede causar un gran impacto en una nación (GFCE, 2017).

Cuando los Estados reconocen este nuevo dominio en el contexto de las sociedades de la información y el conocimiento, la primera estrategia que adoptan es reconocer con cuál ICC cuentan para mantener la operación y gobernabilidad de la nación (Cano, 2011). Es por esto que la falta de controles de ciberseguridad para proteger estos activos origina riesgos para un Estado.

Un criterio importante de las ICC, es que realizan funciones que están respaldadas por la amplia categoría de tecnología, que incluye tecnología de la información (TI), sistemas de control industrial (ICS) y dispositivos conectados en general, incluyendo el Internet de las Cosas (IoT) (NIST, 2018), es decir las ICC hacen parte de las organizaciones que se basan en el funcionamiento correcto de las TIC. Esta dependencia cibernética, es decir de la tecnología, la comunicación y la interconexión, amplía el riesgo potencial para las operaciones. El problema se aumenta cuando una infraestructura es dependiente de otra, con lo que la caída de una supondría la paralización de los servicios de ambas.

Sumado a lo anterior, algunos criterios para la identificación de ICC son: tamaño de la población afectada, dependencia intersectorial, impacto geográfico, seguridad personal, impacto en la privacidad (ENISA, 2014).

Ahora bien, a diferencia de la secuencia lógica para la seguridad de la información que consta de tres objetivos: confidencialidad, integridad y disponibilidad, en el contexto de la ICC, tomando como referencia la importancia de la información, cambia la prioridad en el proceso y el objetivo principal es la disponibilidad; es decir, mantener y garantizar el funcionamiento de todos los componentes, en segundo lugar, la integridad, y la prioridad más baja se da a la confidencialidad, porque los datos circulando en el sistema es constante y su análisis dentro del contexto no es estimable (Erokhin, Petukhov, & Pilyugin, 2019).

Para concluir, aunque para efectos del análisis las IC e ICC, son consideradas sistemas diferentes, en la realidad se encuentran estrechamente relacionadas. Por ejemplo, las IC pueden fallar por muchas razones, y ninguna de ellas están relacionadas con un componente cibernético, las fallas más comunes son: la obsolescencia de su maquinaria y los desastres naturales, como un terremoto o una inundación. Caso opuesto, una falla común en una ICC es causada

principalmente por amenazas cibernéticas (GFCE, 2017). Esto significa que la infraestructura crítica es más susceptible a variedad de riesgos.

3.2 Análisis de la guía para la identificación de las Infraestructuras Criticas Cibernéticas de Colombia.

En el año 2015, el Comando Conjunto Cibernético (CCOCI) de las FF.MM. de Colombia emitió la primera edición de la Guía para la identificación de la ICCC, la cual tiene como propósito definir las actividades para la identificación de la infraestructura Critica Cibernética de Colombia. Su alcance aplica a todas las entidades, públicas, privadas y de economía mixta, que cuenten con infraestructura de TIC dentro del territorio nacional.

La elaboracion de este tipo de guías permite identificar, catalogar y priorizar los servicios esenciales, lo cual conlleva a la protección de las ICCC, permitiendo dar respuesta a las crisis que puedan generarse a causa de sus interrupciones, con el fin de mantener su normal funcionamiento. Es por esto, que los países abordan el problema con diferentes perspectivas y enfoques, centrándose en sus características y prioridades.

En el CCOCI en coordinación con el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, anualmente a través del empleo de la guía se emite un catálogo de ICC de la Nación, con la cual se busca identificar las infraestructuras estratégicas de Colombia, priorizarlas y establecer su grado de vulnerabilidad, los riesgos existentes y las estrategias de mitigación de posibles ataques.

La guía presenta, como se ilustra en la Figura 3, las infraestructuras estratégicas que hacen parte de la totalidad de infraestructuras del país y que se dividen en físicas o cibernéticas. Las infraestructuras cibernéticas según el CCOCI se clasifican en no críticas y críticas, siendo las IC aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su

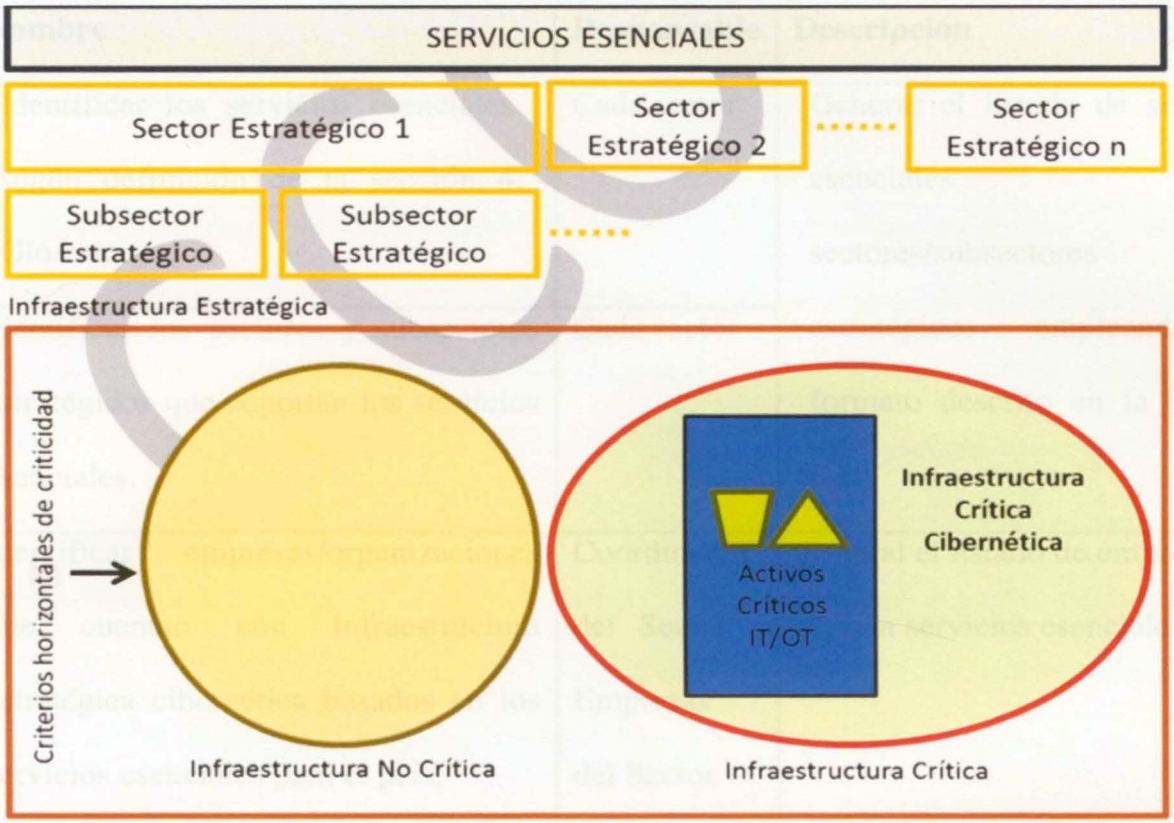
perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España (CCOCI, 2016).

Figura 3. Diagrama de Infraestructura.

Fuente: CCOCI, (2015).

Un marco metodológico para la identificación de los activos críticos se presenta en la Figura 4, en la cual se observa un catálogo con dos secciones: Servicios esenciales e Infraestructura Estratégica. La primera enumera los sectores estratégicos de 1 hasta n sectores y los subsectores estratégicos de cada uno de los sectores. No obstante, si se analiza la gráfica, de los sectores y subsectores se debe desprender los servicios esenciales y no como en ella aparece. En la segunda sección, se divide la infraestructura estratégica en infraestructura no crítica y crítica, con unos criterios horizontales de criticidad, es decir aquellos elementos que nos permiten generar un mejor inventario de los activos que se deben proteger.

Figura 4. Marco Metodológico para la identificación de la ICCC.



Fuente: CCOCI, (2015).

Las actividades que se deben llevar a cabo para identificar las ICCC, no contiene una descripción de las tareas que deberían llevarse a cabo para plena identificación. como se observa en la tabla 4; se puede notar la ausencia de actividades que permitan identificar cada sector, subsector y servicio; tampoco están registradas actividades para identificar las entidades públicas y privadas que pertenecen a la infraestructura crítica del País, entre otras ausencias que el análisis permite notar.

Tabla 4. Actividades para la identificación de la infraestructura critica cibernética.

No	Nombre	Responsable	Descripción
1	Identificar los servicios esenciales, según definición de la sección 4. Glosario.	Cada sector	Generar el listado de servicios esenciales vs. sectores/subsectores estratégicos empleando el formato descrito en la sección 6.2.
2	Identificar los sectores y subsectores estratégicos que soportan los servicios esenciales.	Cada sector	
3	Identificar empresas/organizaciones que cuentan con infraestructura estratégica cibernética basados en los servicios esenciales para el país.	Coordinador del Sector / Empresas del Sector	General el listado de empresas que prestan servicios esenciales.
4	Identificar la infraestructura estratégica cibernética dentro de cada empresa/organización identificada, que soporta los servicios esenciales.	Coordinador del Sector / Empresas del Sector	Generar el listado de infraestructura estratégica cibernética, empleando la taxonomía descrita en la sección 6.3.
5	Aplicar la tabla de variables de criticidad a la infraestructura estratégica cibernética identificada en el punto 4, considerando una afectación tal que impida la prestación	Coordinador del Sector / Empresas del Sector	Diligenciar el catálogo de infraestructura crítica cibernética descrito en la sección 6.4, empleando los criterios horizontales de criticidad descritos

No	Nombre	Responsable	Descripción
	del servicio por causa de la materialización de una amenaza cibernética.		en la sección 6.5.
6	Consolidar el listado de infraestructura crítica cibernética.	CCOC Mesa Nacional	Analizar y depurar la información enviada por los sectores y en caso requerido solicitar aclaraciones o correcciones.
7	Generar catálogo de infraestructura crítica cibernética.	CCOC Mesa Nacional	Consolidar la información enviada por los sectores para generar el catálogo de infraestructura crítica cibernética del País.

Fuente: CCOCI, (2015).

Aun así, los tres criterios horizontales de criticidad que establece el CCOCI para identificar una infraestructura como infraestructura estratégica cibernética, son los siguientes:

a) El impacto social: Valorado en función de la afectación de la población (incluyendo pérdida de vidas humanas), el sufrimiento físico y la alteración de la vida cotidiana, con un valor mínimo del 0,5% de la población nacional.

b) El impacto económico: Valorado en función de la magnitud de las pérdidas económicas en relación con el Producto Interno Bruto de Colombia (PIB), con un valor mínimo de Impacto de 0.123% sobre el PIB Anual.

c) El Impacto medioambiental: Valorado en función de los años que tarda la

recuperación del medio ambiente, con un valor mínimo de impacto de 3 años.

Sobre los criterios dos estudios aportan para su interpretación. El primero el de Fekete (2011) realizó una investigación donde se pudo identificar los criterios mínimos para evaluar una infraestructura critica. En este documento se pueden observar tres criterios de criticidad, denominados proporción critica, tiempo crítico y calidad critica. (Fekete, 2011). El segundo, Theoharidou y otros (2009), quienes coinciden con el primer estudio citado en que los criterios de criticidad más comunes son la proporción de la población afectada, el nivel de Impacto y el efecto en el tiempo. (Theoharidou, Panayiotis Kotzanikolaou y Dimitris, 2009). Con anterioridad a los dos estudios citados, en el año 2006 y 2009, la Unión Europea y los Estados Unidos respectivamente, ya habían establecido los factores para identificar un servicio como crítico, entre los cuales están impacto político, salud pública, entre otros, adicionales a los servicios establecidos por el CCOCI.

Otra situación que genera la necesidad de contar con otros criterios y/o variables que permitan la generación de un inventario no muy amplio de infraestructuras, hacia las cuales se puedan direccionar los presupuestos y medidas de seguridad y protección respectiva, con el fin de garantizar el orden público de la nación, es que la guía solo cuenta con tres criterios daño al medio ambiente, perjuicios económicos y afectación a la población civil para determinar la criticidad de los servicios vitales de la Nación. Se considera que a través de la Guía Metodológica de identificación de ICC, el CCOCI pueda identificar y clasificar la ICCC y de esta manera establecer inventarios y prioridades de protección.

3.3 Análisis de metodologías para la identificación y priorización de las ICC.

Mintzberg (2005) define la metodología cómo "elementos fundamentales que contiene el conjunto de estrategias, procedimientos y acciones organizadas y planificadas por las personas

de la organización, de manera sensata y reflexiva, con la finalidad de posibilitar el cumplimiento de los objetivos generales de la organización". (Mintzberg & Lampel, 2005) P.49

Para entender con mayor detalle la diferencia entre modelo, método, metodología y técnica se presentan sus definiciones en la tabla 5.

Tabla 5. Definición de conceptos.

Elemento	Definición
Modelo	Modelo es la forma en que se concibe que ha de desarrollarse la representación o el arquetipo de una realidad organizacional. Un modelo es la manera que tiene las personas en las organizaciones de considerar como se va a proceder en las actividades o labores encomendadas. Se puede decir que un modelo es la construcción científica bajo la cual se sustenta la realidad de una organización (Mintzberg, 2005). En suma, el modelo es la representación teórica de algo que posteriormente se lleva a la práctica en un contexto concreto.
Método	El método es la manera de poner en práctica el modelo construido. El método se relaciona con un determinado estilo de gerencia que pone en práctica de forma coherente el modelo que se tenga como "creencia". El método posibilita que se desarrollen las actividades que se desarrolle en las organizaciones las prácticas necesarias para la aplicación del modelo descrito (Mintzberg, 2005).
Metodología	Con la metodología se concreta el método en el contexto determinado para la consecución de unos objetivos determinados en función de la realidad empresarial y de las características específicas. Se distingue del método

Elemento	Definición
	porque concreta aún más dependiendo del medio en el que se esté y de los recursos con los que se cuente. La metodología es uno de los elementos fundamentales que contiene el conjunto de estrategias, procedimientos y acciones organizadas y planificadas por las personas de la organización, de manera consciente y reflexiva, con la finalidad de posibilitar el cumplimiento de los objetivos generales de la organización.
Técnica	Las técnicas o estrategias son lo más concreto en la realidad de las aulas. Son la aplicación última del modelo diseñado que desarrollan y aplican las actividades concretas en momentos específicas para determinadas personas.

Fuente: Elaboración propia a partir de Mintzberg, (2005).

La metodología funciona como el soporte conceptual que rige la manera en que aplicamos los procedimientos en una investigación (Hurtado, 2012). Específicamente una metodología, en el marco de objetivos globales y de politicas públicas, busca organizar y estructurar las tareas que comprenden el esfuerzo para lograr objetivos globales; incluir métodos y técnicas para realizar tareas individuales; prescribir un orden en el que se toman ciertas clases de decisiones y, finalmente, prescribe las formas de tomar esas decisiones que conducen a los objetivos deseados (Nance & Arthur, 1988).

Por tanto, si una metodología se convierte en el camino que se debe seguir con el fin del alcanzar un objetivo determinado que se ha trazado, entonces para entender, representar y construir los diferentes modelos que se han planteado en diferentes países para llevar a cabo la identificación de las ICC es necesario conocer las metodologías presentadas en la tabla 6, comúnmente aceptadas para el desarrollo de este tipo de ejercicios con las ICC.

Tabla 6. Relación de metodologías de identificación de ICC.

País u organización	Metodología	Descripción	Fuente
Unión Europea	Metodología para la identificación de activos y servicios de Infraestructura de Información Crítica de ENISA.	Publicada en el 2014, la cual tiene el objetivo de proporcionar una visión general del estado actual de las ICC en Europa y describir posibles mejoras para estar preparados para futuros escenarios de amenazas y desafíos, a través del análisis de diferentes enfoques llevados a cabo por algunos de los Estados Miembro de la Unión Europea para la identificación de la Infraestructura de Información Crítica.	(ENISA, 2014).
Estados Unidos	Programa Nacional de Priorización de Infraestructura Crítica (NCIPP)	Es utilizado por el Departamento de Seguridad Nacional para priorizar la infraestructura crítica. El programa utiliza umbrales de consecuencia basados en fatalidades, pérdidas económicas, duración de la evacuación masiva	(U.S. Goverment Accountability Office, 2013)

País u organización	Metodología	Descripción	Fuente
		y degradación de la seguridad nacional.	
Alemania	Proceso de identificación de siete pasos de la Oficina Federal de Protección Civil y Asistencia de Desastres	Esta herramienta de orientación se basa en un método para identificar infraestructuras críticas, en cooperación con la Oficina Federal de Seguridad de la Información de Alemania (BSI). Este método utiliza enfoques ya existentes y los combina de manera inteligente. El método de identificación se basa en tres criterios ellos son: calidad, cantidad y tiempo.	(Federal Office of Civil Protection and Disaster Assistance (BBK), 2017)
Republica Checa	Reglamento del gobierno de la república checa no. 432/2010. Acerca de los criterios para	Las IIC se identifican mediante un proceso específico de conformidad con la Ley núm. 240/2000. A través de criterios como: (1) Si	(Harasta, J, 2018).

País u organización	Metodología	Descripción	Fuente
	determinar los elementos de infraestructura crítica	causa la muerte de más de 250 personas, (2) la economía del estado está dañada por más del 0,5% del PIB, o tiene un grave impacto en la provisión servicios necesarios para más de 125,000 personas.	
Reino Unido	El marco estratégico para la resiliencia de la infraestructura crítica	La infraestructura se clasifica según su valor o "criticidad", incluye tres dimensiones de impacto: (a) impacto en la entrega de los servicios esenciales de la nación; (b) impacto económico (derivado de la pérdida de servicios esenciales); y (c) impacto en la vida (derivado de la Pérdida de servicios esenciales).	(Sharma, 2017)
Lituania	Metodología de identificación de Infraestructuras	La importancia de la infraestructura se determinará en función del daño potencial	(Lietuvos Respublikos Vyriausybe, 2016).

País u organización	Metodología	Descripción	Fuente
	Criticas de la Información	causado, se tendrán en cuenta algunos de los siguientes criterios: (1) influencia en la interrupción de la provisión de un servicio crítico; (2) peligro para la vida y la salud de la población; (3) daño económico al estado; (4) daño ambiental; (5) confianza de la población en el estado; (6) la influencia de una infraestructura en otra infraestructura, entre otros.	
Fuerza Aérea Colombiana	"360-DEGREE-FEEDBACK Instrumento metodológico para identificar, catalogar y priorizar los servicios críticos de una nación.	Es un instrumento metodológico para identificar, catalogar y priorizar los servicios críticos de una nación. Esta metodología ofrece un marco teórico, llamado: "360-DEGREE-FEEDBACK", el cual contiene 8 etapas y 3 categorías principales. Una de las características principales es que los países no necesitan haber	(Herrera L. C., 2019).

País u organización	Metodología	Descripción	Fuente
		identificado las IC antes de la aplicación de este método.	

Fuente: Elaboración propia a partir de metodologías revisadas, (2020).

A la luz de la documentación revisada y según los aportes que estas generan para la identificación de las ICCC, la metodología a tener en cuenta para el desarrollo de la actualización objeto del presente trabajo, es la propuesta por ENISA, porque permite llevar con mayor detalle la identificación de ICC. También será abordadas de manera detallada a continuación un instrumento metodológico para identificar, catalogar y priorizar los servicios críticos de la Nación utilizado por la Fuerza Aérea de Colombia.

El documento metodología para la identificación de activos y servicios de la ICC para los países miembros de la Unión Europea (EU), publicado en 2014 por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) se fundamenta en la información recopilada de algunos Estados miembros, los cuales han adelantado el proceso de identificación de los servicios críticos y sus activos. Uno de los lineamientos que emite la metodología es proporcionar una lista de once sectores críticos para la EU de acuerdo con las características propias de la región.

En el documento de ENISA se identifican dos enfoques metodológicos utilizados por algunos países. En primer lugar, el enfoque "Dependiente del Servicio No-Crítico"; este enfoque se basa principalmente en el análisis de la arquitectura de red, la cual es una metodología que, aunque no se utiliza en ningún país miembro de la EU a nivel gobierno, para las empresas es una herramienta que es utilizada para mapear sus redes de datos y comunicaciones. Este enfoque

incluye: el análisis de la red de datos e IP, los patrones de carga de tráfico y los patrones de falla y la identificación de componentes, que son críticos para el funcionamiento de la red en general o de una parte importante de la red. El objetivo principal de este enfoque es generar un mapa global, a través de la identificación de la red central de datos y comunicaciones, y un mapa de aquellos componentes adicionales que una organización utiliza durante el tráfico de datos. Una de las desventajas es que se debe diseñar un mapa completo de la arquitectura de la red, ignorando por completo los servicios críticos que están interconectados a través de las TIC, porque se basa específicamente en la infraestructura de la red en su conjunto y no en la criticidad de los servicios. (Mattioli, 2014).

En segundo lugar, ENISA menciona el enfoque "Dependiente del Servicio Crítico"; esta metodología presenta tres pasos principales para la identificación, priorización y catalogación de los servicios críticos.

El primer paso es la identificación del sector crítico, en esta fase, los Estados miembros ya han identificado una lista de sectores de CI, es importante resaltar que este proceso ya fue cumplido al 100% por los países miembros de la UE.

El segundo paso es la identificación de servicios críticos, la cual se divide en dos sub-enfoques, cada uno de los cuales es responsable de identificar los servicios críticos: el primer sub-enfoque es el direccionado por el Estado, en éste el Estado, a través de las agencias gubernamentales, es el responsable de identificar los sectores críticos y la lista de servicios esenciales, en este paso el gobierno nacional selecciona a los operadores que son responsables de proporcionar estos servicios esenciales; el segundo sub-enfoque es el direccionado por el operador de la IC, en éste el operador es el responsable de identificar los activos y servicios de ICC, de acuerdo con los sectores críticos y los criterios de criticidad establecidos a nivel

nacional.

El tercer paso es la identificación de los activos y servicios de la red de infraestructura de información crítica que respaldan los servicios críticos, los cuales deben ser identificados al detalle a través de los criterios de criticidad establecidos previamente a nivel nacional. En esta fase final cada operador de IC debe establecer como mínimo un plan de protección respectivo para cada servicio identificado como crítico.

ENISA recomienda más criterios a ser tenidos en cuenta por parte de los Estados miembro de la EU, para la identificación de las sus ICC, tomando como referencia lo que había sido emitido por la EU y como manera de poner a disposición más elementos para la identificación. Estos criterios son:

1. Población afectada (el porcentaje de la población de afectada por la interrupción del servicio).
2. Concentración (la densidad de la población en el área geográfica que se afecta interrupción del servicio).
3. Impacto económico (el costo de la interrupción del servicio en términos de porcentaje del PIB).
4. Confianza pública (el efecto que el funcionamiento adecuado de este servicio tiene en la confianza pública hacia el gobierno).
5. Relaciones internacionales (el efecto que tendrá una interrupción del servicio en las relaciones entre el Estado y otros países).
6. Orden público (el efecto que una interrupción del servicio puede causar al orden público).
7. Operaciones públicas obstaculizadas (las operaciones diarias del público, como ir a

trabajar en transporte público, se detienen o se frustran).

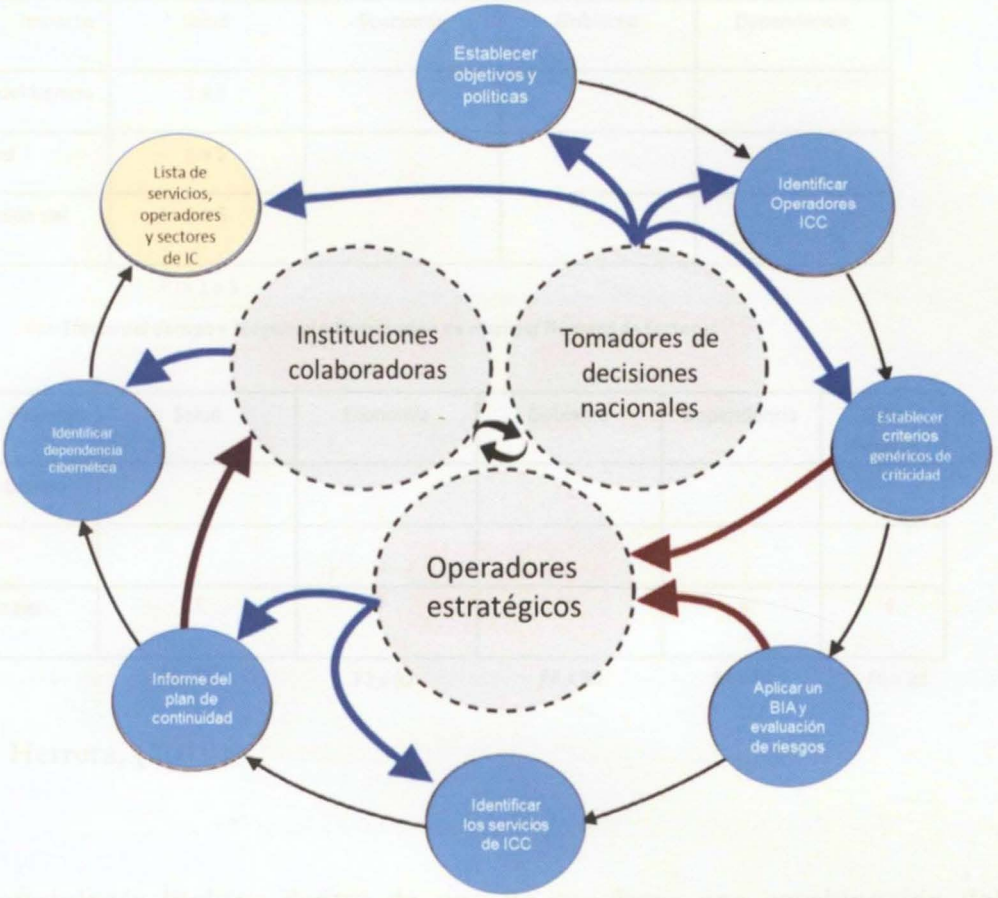
8. Los servicios de otros países se ven afectados (las interdependencias con servicios críticos de otros Estados deben tenerse en cuenta) (ENISA, 2014, p.24).

Otro ejemplo de herramientas disponibles para la identificación de sectores, subsectores y servicios esenciales es la metodología publicada por la Fuerza Aérea Colombiana y la Universidad Tecnológica de Tallin (Estonia) en la revista científica "Elsevier" en febrero del 2019. En esta publicación se presentó un instrumento metodológico para identificar, catalogar y priorizar los servicios críticos de una nación. Esta metodología ofrece un marco teórico, llamado: "360-Degree-Feedback", el cual contiene ocho etapas y tres categorías principales.

Una de las características principales es que los países no necesitan haber identificado las IC antes de la aplicación de este método, debido a que una vez que se identifican los servicios esenciales, cada uno de ellos contiene la ruta a recorrer en el proceso, tal como operadores, subsectores y sectores (Herrera L. C., 2019).

Como se ilustra en la figura 5, la metodología creada por la Fuerza Aérea Colombiana está organizada en dos partes principales; la primera se centra en la identificación de los stakeholders o partes interesadas, con el fin de permitir el diseño de políticas y directrices nacionales para la distribución de tareas. Esta parte se clasifica en tres capas que interactúan entre sí: tomadores de decisiones nacionales; operadores estratégicos; e instituciones colaborativas.

Figura 5. Ilustración de la metodología para la identificación de los servicios críticos.



Fuente: Herrera, (2019).

La segunda parte visualiza el marco de 360-Degree-Feedback, el cual tiene como finalidad recopilar datos generados por los stakeholders, el cual contiene ocho pasos específicos e incluye un proceso de cálculo para la clasificación de criticidad que funciona como una matriz ajustable, como se ilustra en la figura 6, donde cada criterio con su rango de tiempo, nivel de gravedad y distribución del alcance, permiten determinar el grado de influencia (ENISA, 2014) y adaptar sus porcentajes o proporciones, dependiendo de las necesidades nacionales.

Figura 6. Matriz para la identificación de los servicios críticos.

Impacto / Factor	Salud	Economía	Gobierno	Dependencia
Efectos del tiempo	1 a 5			
Magnitud	1 a 5			
Distribución del Alcance	1 a 5			

R1= 1 a 5

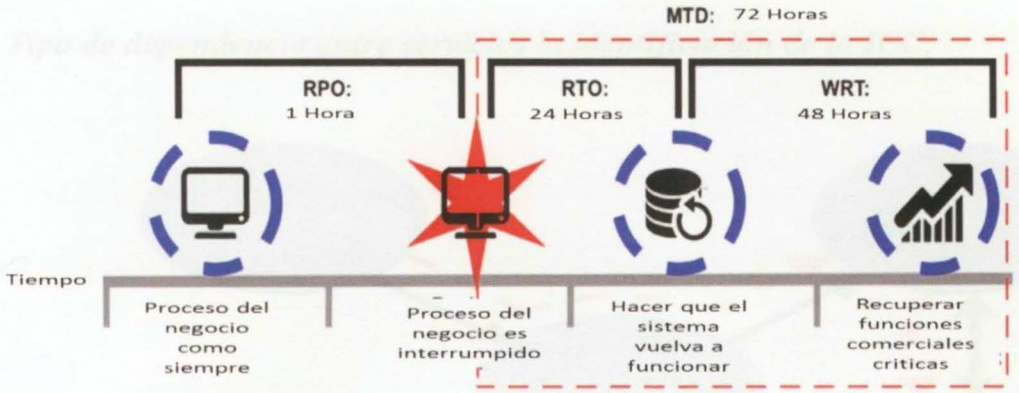
R1= Efecto del tiempo + Magnitud + Distribución de alcance/ Número de Factores

Impacto / Factor	Salud	Economía	Gobierno	Dependencia	Otro impacto
Efectos del tiempo					
Magnitud					
Distribución del Alcance					
	P1 x R1	P2 x R2	P3 x R3	P4 x R4	P5 x R5

Fuente: Herrera, (2019).

Esta metodología incluye dentro de uno de sus fases una combinación del análisis de impacto de negocios y la evaluación de riesgos con el fin de correlacionar los servicios empresariales esenciales y amenazas potenciales; el propósito de esta etapa es que los operadores de infraestructura crítica estimen el impacto del tiempo de inactividad de cada servicio esencial y los elementos que se verían afectados después de la interrupción; como resultado de esta combinación, cada operador de ICCC puede establecer un plan de continuidad interno que incluye un análisis del impacto financiero y el impacto operativo del servicio, como una estrategia de mitigación, tal como se ilustra en la Figura 7.

Figura 7. Análisis de impacto de negocios la identificación de los servicios crítico.



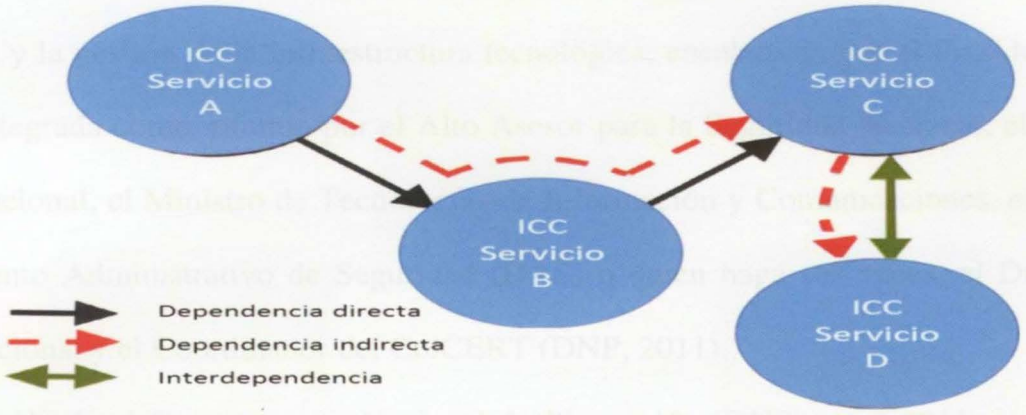
Fuente: Herrera, (2019).

Otra ventaja de la metodología es la fase de dependencia entre los servicios críticos que están en proceso de identificación; los efectos catastróficos de forma recursiva en las infraestructuras interconectadas, incluso sí la probabilidad de ocurrencia es baja; el resultado de esto puede ser devastador para múltiples servicios y puede causar una falla en cascada en los sistemas de información. En la Figura 8 se muestran los tres tipos de dependencia que se podrían establecer durante esta fase.

Ahora bien, las dos metodologías tienen en común que nos llevan a reconocer la importancia de la participación del sector gobierno y del sector privado durante la identificación de la ICCC; adicionalmente ENISA aporta un aspecto a tener en cuenta en la utilización de la metodología 360-Degree-Feedback: el amplio número de criterios que sirven para la definición de las ICC; donde cada criterio seleccionado por las partes interesadas en la identificación, reciben un valor de acuerdo a la importancia de su servicio, para posteriormente ser puestos en consideración, con el factor de rango de tiempo, nivel de gravedad y distribución del alcance del

impacto del enfoque 360-Degree-Feedback; este proceso permite determinar el grado de influencia en las afectaciones que se puedan presentar.

Figura 8. Tipo de dependencia entre servicios la identificación de la ICC.



Fuente: Herrera, 2019

En conclusión, estas metodologías pueden favorecer la identificación de las ICCC, obteniendo de manera más precisa y rigurosa el inventario de activos hacia los cuales se deben direccionar los esfuerzos y presupuestos para protección; por lo tanto, se consideran en el presente estudio como aportes significativos para llevar a cabo la actualización de la guía metodológica de ICCC.

3.4 Análisis de los Organismos Involucrados en el Proceso de Identificación de la ICCC

Para identificar la ICCC se requiere establecer la definición de las partes interesadas o entes involucrados en el proceso y la terminología usada para este efecto. Esto puede ser determinado a través de dos vías: (a) las políticas emitidas por el Gobierno Nacional en el año 2011 (DNP, 2011), para fortalecer las capacidades del Estado y afrontar las ciberamenazas que atentan contra la seguridad y defensa en el ciberespacio; (b) las recomendaciones formuladas en

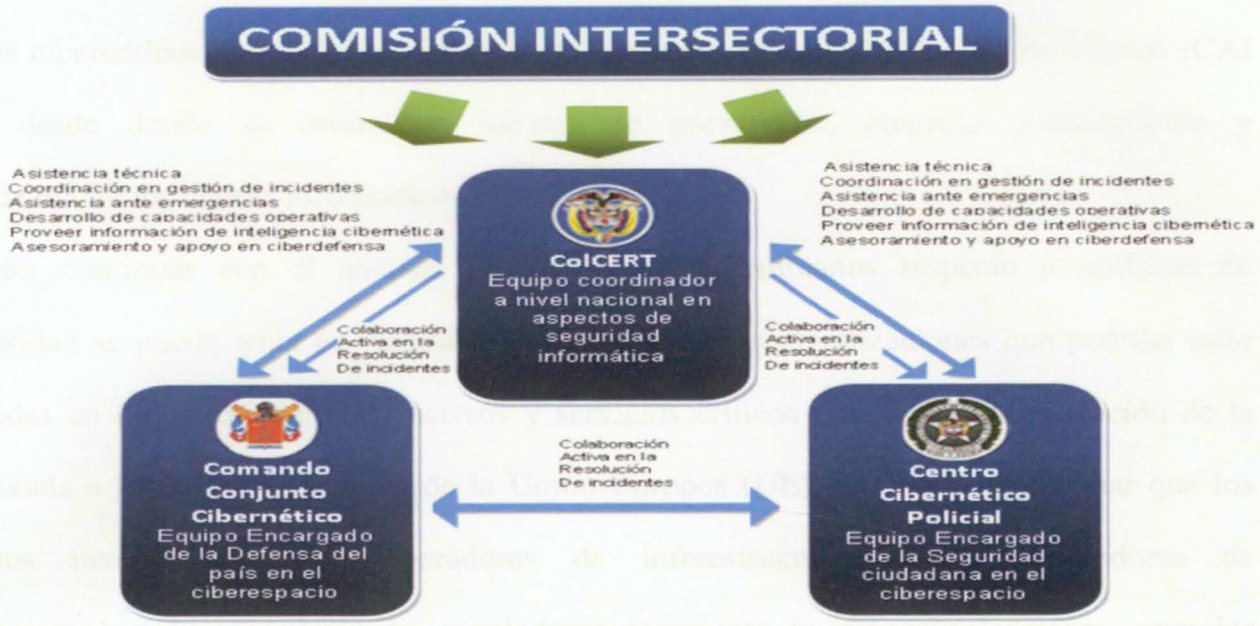
las metodologías y enfoques existentes, tales como: Fuerza Aérea Colombiana (FAC) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

En cuanto a las políticas emitidas por el Estado, el CONPES 3701 da cuenta de la creación de una comisión intersectorial encargada de establecer la estrategia nacional de la ciberseguridad y la gestión de la infraestructura tecnológica, encabezada por el Presidente de la República e integrada como mínimo por el Alto Asesor para la Seguridad Nacional, el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director del Departamento Administrativo de Seguridad (DAS) o quien haga sus veces, el Director de Planeación Nacional y el Coordinador del ColCERT (DNP, 2011).

Aunque desde el Departamento Nacional de Planeación (DNP) en el 2011, se diseñó la política y se conformaron los entes regulatorios para la identificación de la ICCC, a la fecha esta iniciativa no es completamente efectiva ya que entidades como el DAS no existen y la IC de Colombia aún no está identificada en su totalidad; pero una de las ventajas de generar el documento CONPES mencionado es la creación del modelo de coordinación nacional entre tres organismos del Ministerio de Defensa Nacional, como se muestra en la figura 9, y también establecer que el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT) es el ente coordinador para los asuntos de ciberseguridad y ciberdefensa en el País, sirviendo como apoyo y soporte a otros organismos, tales como: el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCOCI).

Es también un logro que a través de este CONPES se asignara al Comando General de las Fuerzas Militares un nuevo rol y consolidar el Comando Conjunto Cibernético (CCOCI), que tiene como principal función prevenir, contrarrestar y mitigar toda amenaza o ciberataque que afecte los intereses del Estado.

Figura 9. Modelo de Coordinación Nacional.



Fuente: CCOCI, (2015).

Es importante resaltar algunas de las funciones asignadas al CCOCI:

a) *Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa.*

b) *Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia.*

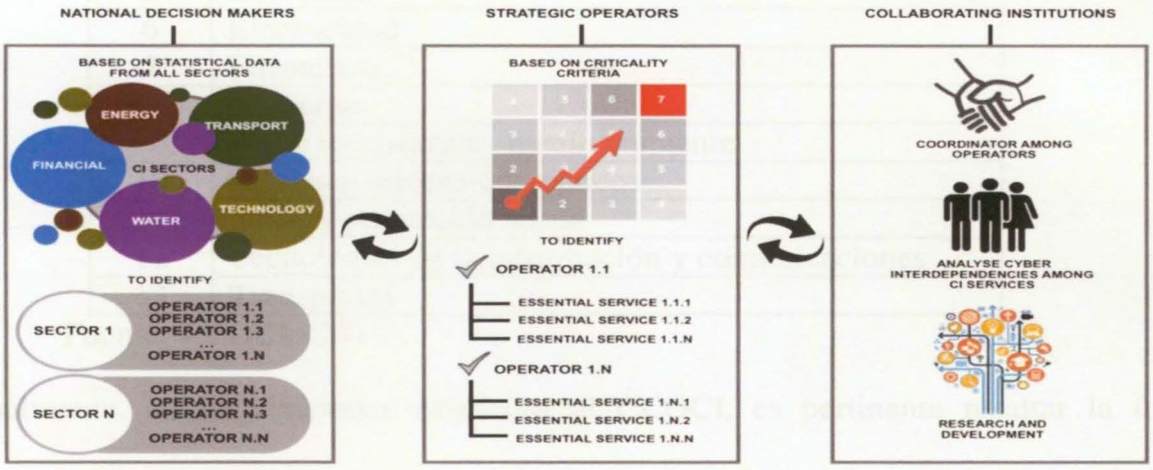
c) *Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional. (DNP, 2011).*

A la Policía Nacional, mediante el Centro Cibernético Policial (CCP), se le asignó liderar los procesos de ciberseguridad en el territorio colombiano y la protección de la ciudadanía ante los delitos cibernéticos, para ello se fortalece el Comando de Atención Inmediata Virtual (CAI Virtual), desde donde se centralizan labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país.

Para continuar con el análisis de los logros colombianos respecto a políticas de ciberseguridad se puede tener en cuenta la encuesta sobre las organizaciones que podrían estar involucradas en la identificación de activos y servicios críticos durante la identificación de la ICC realizada a los países miembros de la Unión Europea (UE), que pudo determinar que los organismos involucrados son: operadores de infraestructura crítica, proveedores de comunicación electrónica, autoridades reguladoras nacionales de telecomunicaciones, agencias de ciberseguridad. (Mattioli, 2014).

Además de lo expuesto, las metodologías y enfoques existentes permiten hacer el análisis académico de los organismos que interactúan durante la identificación de la Infraestructura Crítica Cibernética de un País. En el caso de ENISA, se precisa que los operadores de cada infraestructura son responsables de determinar la identificación de los activos de red que se utilizan para operar las aplicaciones de los servicios críticos. En esta metodología se considera un activo crítico en relación con: el valor comercial, el alcance de la población atendida, la dependencia técnica de las aplicaciones críticas. Usando las metodologías 360-Degree-Feedback, de la FAC, y la de identificación de activos y servicios de ICC de ENISA se obtienen algunos organismos, como los expuestos en la figura 10.

Figura 10. Partes interesadas en la identificación de la ICC.



Fuente: Herrera, (2019).

Hay que mencionar ademas que en Colombia, a través de un trabajo conjunto con el personal experto del gobierno, Fuerzas Militares, la academia y empresas del sector público y privado, se identificaron trece (13) Sectores nacionales con sus respectivos subsectores, con quienes constantemente se llevan a cabo diferentes mesas de trabajo, con el fin de analizar y generar nuevas iniciativas de protección para las infraestructuras, tomando como referencia las diferentes lecciones que se presentan a nivel nacional e internacional y así mismo son los que suministran la información necesaria acerca de sus ICC, para poder llevar a cabo el proceso de identificación. Los sectores identificados en Colombia, publicados en la cartilla "Sectores Estratégicos de la República de Colombia desde la Óptica Cibernética" son los que se relacionan en la tabla 7, así:

Tabla 7. Sectores estratégicos de Colombia.

No	Sector
1	Alimentación y agricultura
2	Agua
3	Comercio, industria, turismo

No	Sector
4	Defensa
5	Educación
6	Electricidad
7	Financiero
8	Gobierno
9	Recursos naturales-medio ambiente
10	Recursos minero-energéticos
11	Salud y protección social
12	Tecnologías de la información y comunicaciones
13	Transportes

Fuente: CCOCI, (2016).

Finalmente, de las funciones asignadas al CCOCI, es pertinente resaltar la función relacionada con la defensa la infraestructura crítica y la minimización de los riesgos informáticos, por cuanto genera la responsabilidad de liderar los procesos y crear herramientas como la Guía Metodológica para la Identificación de las ICC, de modo que se ejecuten actividades de ciberdefensa de las infraestructuras; para lo cual se hace necesaria la participación de todos los sectores que integran los servicios esenciales y sus respectivos operadores, con el fin de obtener la información suficiente y necesaria de sus activos, a partir de los cuales se implementa la metodología que permita su identificación, priorización y protección.

3.5 Propuestas de valor para la protección de las ICC, a través de su identificación.

Hasta aquí, el análisis de la información permite inferir y resaltar que la importancia de una IC se hace evidente y más visible en caso de falla, cuando los servicios que esta ofrece ya no están disponibles imprevistamente; por lo que contar con elementos que agilicen su identificación y control es esencial, más aún teniendo en cuenta que los sistemas de información han convertido a gran parte de las IC en ICC, pero además, aunque las fallas más comunes de las IC son la obsolescencia de su maquinaria y los desastres naturales, las TIC se constituyen en uno de los elementos más importantes a la hora de proteger IC de servicios vitales para la sociedad.

Es decir, dado que la interdependencia informativa que se genera entre diferentes infraestructuras, la vulnerabilidad de la ICC tienen un efecto significativo y hasta total en el funcionamiento de una IC, por lo que su protección es determinante; entonces, las ICC se constituyen en elemento esencial en la actualidad para el eficaz y efectivo desempeño de los servicios necesarios para el buen funcionamiento de un país, de una ciudad o de cualquier organización; así es que la no disponibilidad de un servicio esencial amenaza la supervivencia o la viabilidad de un sector y al mismo tiempo de los sectores que dependan de él de manera directa o indirecta.

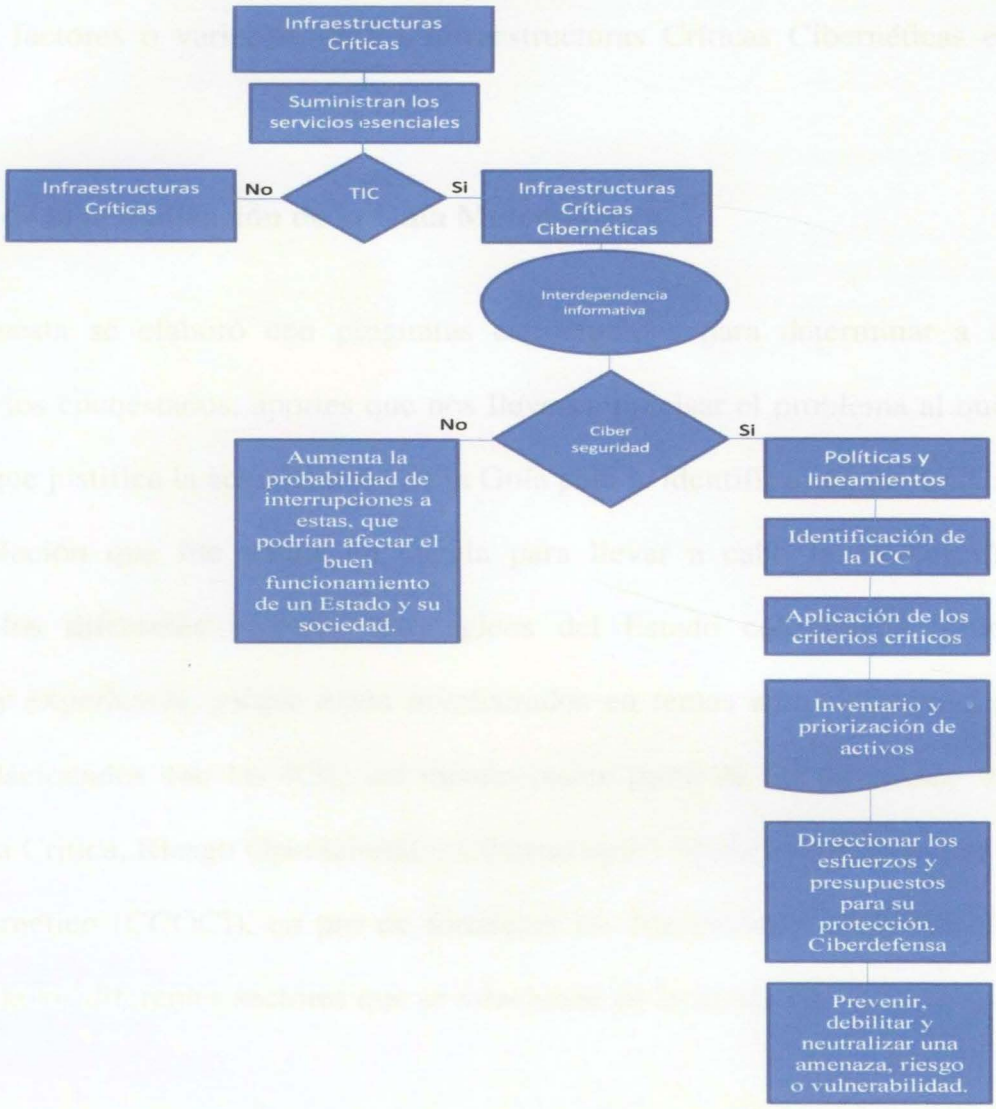
La falta de controles y herramientas integrales de ciberseguridad para proteger las ICC, conlleva a que la ciberdefensa sea una capacidad no funcional, lo que origina un grave riesgo para un Estado. Por lo tanto, un Estado debe considerar la identificación, catalogación y priorización de la ICC como un elemento esencial para formular estrategias, políticas, lineamientos y guías en pro de su protección y aseguramiento. Además de responder a razones de seguridad nacional la identificación, catalogación y priorización de las ICC contribuye a la reducción de tiempo en el desarrollo de los procesos y está fundamentada en consideraciones financieras.

Es así que, para obtener de manera más precisa y rigurosa el inventario de activos hacia los cuales se debe direccionar los esfuerzos y presupuestos para la protección de ICC, las metodologías y enfoques para identificar, catalogar y priorizar las ICC, se acogen a criterios tales como población afectada, concentración, impacto económico, confianza pública, orden público, interdependencia, en búsqueda de garantizar la funcionalidad, continuidad e integridad de las ICC y de esta manera prevenir, debilitar y neutralizar una amenaza, riesgo o vulnerabilidad.

Fuente: Elaboración Propia, (2020).

Para lo cual se hace necesaria la participación de los diferentes sectores suministrando la información necesaria y de manera rigurosa al CCOCI, con el fin de diseñar las estrategias pertinentes de mitigación y monitoreo del estado operativo de las infraestructuras. Como resultado final, a través del flujograma en la figura 11, se resalta la necesidad de la protección e identificación de las ICC.

Figura 11. Flujograma para la protección e identificación de las ICC.



Fuente: Elaboración Propia, (2020).

Capítulo IV

Identificación de las características, criterios o variables de las ICC.

En este capítulo se expone la aplicación del método de recolección de datos primarios, usando la visión y experiencia de los profesionales expertos en la protección de las ICCC, a través de dos encuestas, la primera para identificar la necesidad de la actualización de la Guía Metodológica para la Identificación de las ICC de la nación y la segunda para identificar características, factores o variables de las Infraestructuras Críticas Cibernéticas en Colombia (ICCC).

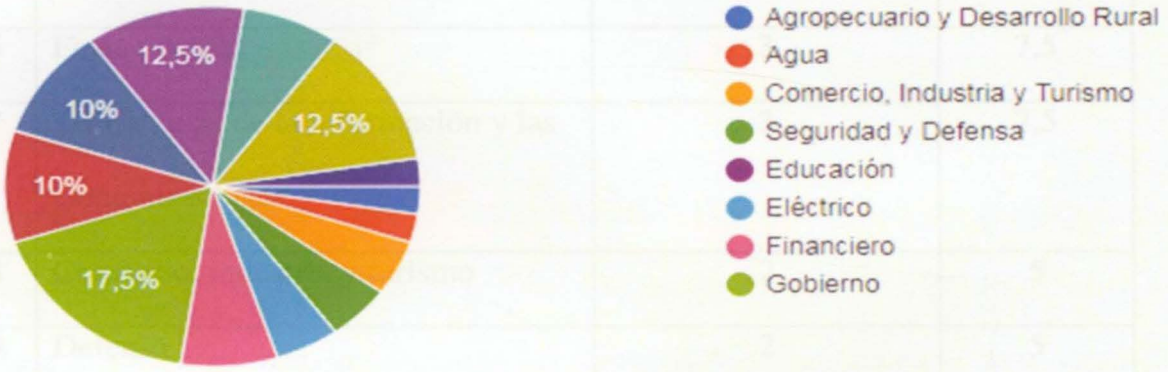
4.1 Necesidad de la actualización de la Guía Metodológica

La encuesta se elaboró con preguntas estructuradas para determinar a través de la experiencia de los encuestados, aportes que nos lleven a precisar el problema al que nos vemos enfrentados y que justifica la actualización de la Guía para la identificación de ICCC.

La población que fue tenida en cuenta para llevar a cabo la recolección de datos, pertenecen a los diferentes sectores estratégicos del Estado colombiano, quienes poseen conocimiento y experiencia porque están involucrados en temas administrativos, operativos y académicos relacionados con las ICC; así mismo hacen parte de las diferentes reuniones de "Infraestructura Critica, Riesgo Operacional y Ciberdefensa" evento organizado por el Comando Conjunto Cibernético (CCOCI), en pro de fortalecer los lineamientos CONPES. Los expertos hicieron parte de los diferentes sectores que se relacionan en la figura 12.

El personal de 40 expertos, fueron encuestados durante el desarrollo de la reunión 67 de la comisión citada; esta primera encuesta[5], se diligenció a través de mesas de trabajo, aportando elementos importantes para el desarrollo de la presente investigación. La encuesta tenía como objetivo conocer la posición con referencia a la necesidad de actualización de la Guía Metodológica de ICC de Colombia del año 2015, la cual tiene un enfoque para la identificación de las ICC, basado en tres criterios horizontales de criticidad.

Figura 12.Porcentaje de encuestados por sectores estratégicos de la ICCC.



Fuente: Encuesta personal de expertos, (2019).

En la tabla 8, se relaciona el número de encuestados por sector estratégico, sectores que se encuentran definidos en los lineamientos de la cartilla sectores estratégicos de la república de Colombia desde una óptica cibernética, del CCOCI, algunos sectores con mayor representación que otros, aspecto que incide al establecer la necesidad de actualización de la guía metodológica para la identificación de la ICC de Colombia 2015.

---

[5] Cuestionario en medio de la reunión No 67 de "Infraestructura Critica, Riesgo Operacional y Ciberdefensa", Tanque de pensamiento para la actualización de la Guía Metodológica de identificación de las ICC de Colombia https://forms.gle/hVC3asA5yiz2eHDJ6

Tabla 8.Porcentaje expertos por sectores estratégicos de la ICC.

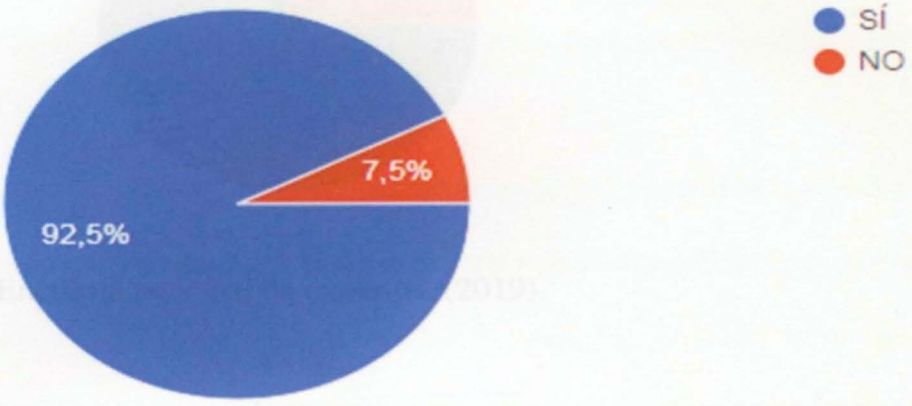
Nro.	Sector	Expertos por sector	Porcentaje
1	Gobierno	7	17,5
2	Salud	5	12,5
3	Transporte	5	12,5
4	Recursos Naturales – Medio ambiente	4	10
5	Recursos Energéticos	4	10
6	Financieros	3	7,5
7	Tecnologías de la información y las Comunicaciones	3	7,5
8	Comercio, industria y turismo	2	5
9	Defensa	2	5
10	Eléctrico	2	5
11	Justicia	1	2,5
12	Agropecuario y desarrollo rural	1	2,5
13	Agua	1	2,5

Fuente: Elaboración propia, (2019).

Con respecto a la pregunta, ¿Considera necesaria la actualización de la Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia desarrollada en el 2015?, en la figura 13, se ilustra que el 92,5% del personal participante en la mesa de trabajo, considera necesaria la actualización, mientras que el 7,5% manifiesta que no es necesaria dicha actualización. Lo anterior nos permite inferir que pueden existir falencias en el proceso de la

identificación, generando vulnerabilidades, al no contar con un inventario claro y adecuado, lo cual genera desgastes en la protección de las ICC.

Figura 13. Porcentaje de expertos que consideran necesaria la actualización de la Guía.

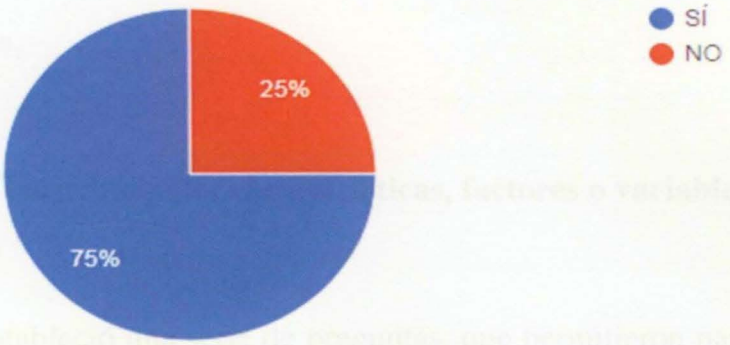


Fuente: Encuesta personal de expertos, (2019).

Con la segunda pregunta de la encuesta se pretendió obtener información que permita un mejor análisis sobre los criterios actuales de la Guía Metodológica para la Identificación de las ICC: ¿Considera que los tres criterios de criticidad horizontal planteados en la guía requieren alguna modificación o ser eliminados?

En la figura 14, se registran las respuestas a la pregunta 2: el 75% de los encuestados consideran la necesidad de modificar los criterios actuales y un 25% consideran que no es necesario. Este resultado nos indica que es ineludible el trazado de ajustes o nuevos criterios, los cuales están limitados al impacto sobre la economía, la población o/y el ambiente, pero no contempla efectos de la duración o del espacio de cobertura del ataque o incidente. Este aspecto es crítico si se considera el riesgo que corre la sociedad por falta de protección o medidas eficientes.

Figura 14. Porcentaje de expertos que piensan que los criterios deben ser modificados.



Fuente: Encuesta personal de expertos, (2019).

En la tercera pregunta, los encuestados ampliaron su percepción frente a la segunda pregunta: ¿Si su respuesta anterior fue SÍ, por favor indique cuál o cuáles criterios, y explique qué tipo de modificación plantea? Las respuestas permiten analizar cuáles son los cambios que deben realizarse: (a) la necesidad de revisar los valores mínimos actuales, (b) tener en cuenta los efectos de la duración o el espacio de cobertura del ataque o incidente (c) incluir nuevos criterios relacionados con gobierno, regulación y reputación (d) la importancia de la interdependencia, la cual genera afectación entre los sectores, a raíz de la conexión informativa que se genera entre diferentes infraestructuras.

En conclusión, esta primera encuesta evidencia la necesidad de la actualización de la Guía Metodológica para la Identificación de las ICC de Colombia; contemplando nuevos criterios; aspecto que es de suma importancia por cuanto de ellos depende que el Estado pueda determinar la importancia de algunas infraestructuras dentro de los diferentes sectores, tanto en circunstancias normales o durante emergencias. Permitir identificar la ICC es crucial para un Estado o específicamente para una IC, Sin embargo, los criterios que son empleados en la guía

metodológica para la identificación de ICC, para evaluar las consecuencias perjudiciales no permiten comprender adecuadamente impactos importantes la interdependencia entre diferentes infraestructuras críticas.

4.2 Identificación de las principales características, factores o variables de las ICCC.

Este método estableció una serie de preguntas, que permitieron parametrizar los criterios y los factores que influyen en cada uno de los aspectos indagados. Esta encuesta fue realizada con el apoyo del CCOCI, unidad a través de la cual fue enviada la encuesta a personal de expertos en ICC. El personal encuestado fue codificado de acuerdo con la siguiente tabla, con el fin de evitar la divulgación de información sensible del sector público y privado que participa en la identificación de la ICCC.

Tabla 9. Codificación del personal encuestado representantes de la ICCC.

Código Encuestado	Compañía que pertenece	Enfoque Académico	Enfoque Operacional
ICC-001	Davivienda		X
ICC-002	Uniandes	X	
ICC-003	Finagro		X
ICC-004	Sociedad de activos especiales		X
ICC-005	Isa – interconexion electrica		X
ICC-006	Ideam		X
ICC-007	Politécnico gran colombiano	X	
ICC-008	Xm – gestión de sistemas		X
ICC-009	Minjusticia		X
ICC-010	Mintic-1		X
ICC-011	Agencia nacional de hidrocarburos		X

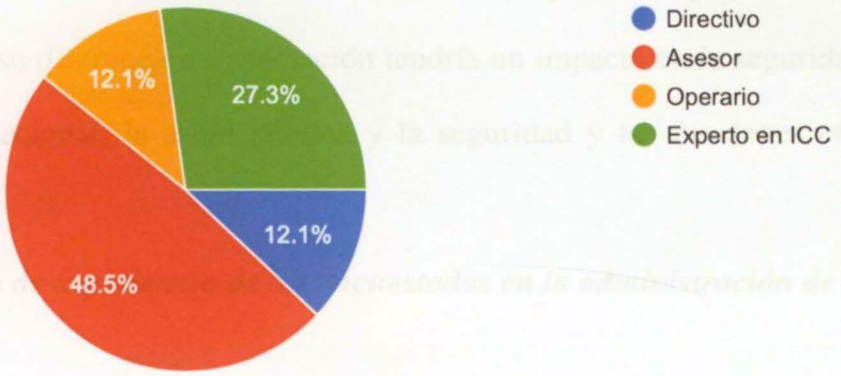
Código Encuestado	Compañía que pertenece	Enfoque Académico	Enfoque Operacional
ICC-012	Cámara colombiana de informática y Telecomunicaciones		X
ICC-013	Mintic-2		X
ICC-014	Supersolidaria		X
ICC-015	Minhacienda		X
ICC-016	Minvivienda		X
ICC-017	Superintendencia de industria y comercio		X
ICC-018	Intercolombia		X
ICC-019	Everis		X
ICC-020	Acis		X
ICC-021	Auditoría general de larepública		X
ICC-022	Esdegue	X	
ICC-023	Dian		X
ICC-024	Scotiabank		X
ICC-025	Minagricultura		X
ICC-026	Agencia nacional de minería		X
ICC-027	Junta central de contadores		X
ICC-028	Fuerza aérea colombiana		X
ICC-029	Ean	X	
ICC-030	Agencia nacional de infraestructura		X
ICC-031	Comisión de regulación de agua potable y saneamiento		X
ICC-032	Ecopetrol		X
ICC-033	Fiscalia		X

Fuente: Elaboración propia, (2020).

Las 33 personas que respondieron a la encuesta, que fue enviada a través del Comando Conjunto Cibernético (CCOCI), representan a los especialistas con conocimientos y experiencias en el campo de las Infraestructuras Críticas, los cuales son representantes del sector privado y

público del país, que participan en la mesa de trabajo de identificación y protección de ICCC, quienes pertenecen el 12.1% al nivel Directivo, el 48.5% se desempeña como asesor, el 12.1% como operario y 27.3% son expertos en ICC, Como se ilustra en la figura 15 esta herramienta[6] fue aplicada mediante dos enfoques (académico y operacional).

Figura 15. Porcentaje de encuestados por niveles de la ICC.



Fuente: Encuesta personal de expertos, (2020).

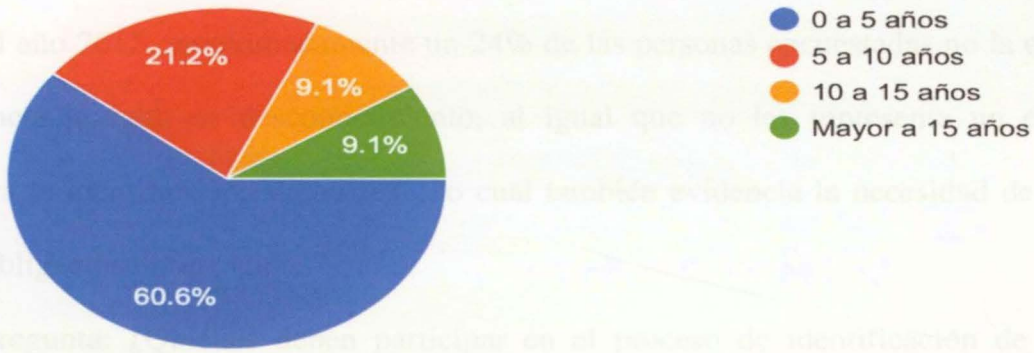
Con relación a la experiencia de cada uno de los participantes en la identificación, catalogación y priorización de la ICCC, se pudo identificar que el 60.6% del personal encuestado tiene una experiencia entre 0 a 5 años, con un 21.2% del personal dice tener de 5 a 10 años de experiencia como operador y/o administrador de ICC, un 9.1% de los encuestados afirma tener entre 10 a 15 años de experiencia, y un 9.1% dice tener más de 15 años trabajando en el sector de las ICC, como se visualiza en la figura 16. Se evidencia que los expertos poseen conocimientos

[6] Cuestionario para el diseño de una guía metodológica que permita la identificación de la Infraestructura Crítica Cibernética de Colombia. https://forms.gle/LAC5DFnZoes5yZS78

actualizados y habilidades para proporcionar criterios y parámetros sobre el asunto de análisis. Se pudo establecer que los encuestados definen las infraestructuras críticas cibernéticas, como:

- Todo componente tecnológico o servicio que pertenece a una IC.
- Infraestructuras tecnológicas que apoyan el logro de los objetivos estratégicos de las entidades en particular y del Estado en general.
- Instalaciones, sistemas de información, servicios públicos que son vitales para una nación que su destrucción o afectación tendría un impacto en la seguridad nacional, la economía nacional, la salud pública y la seguridad y las funciones efectivas de un Estado.

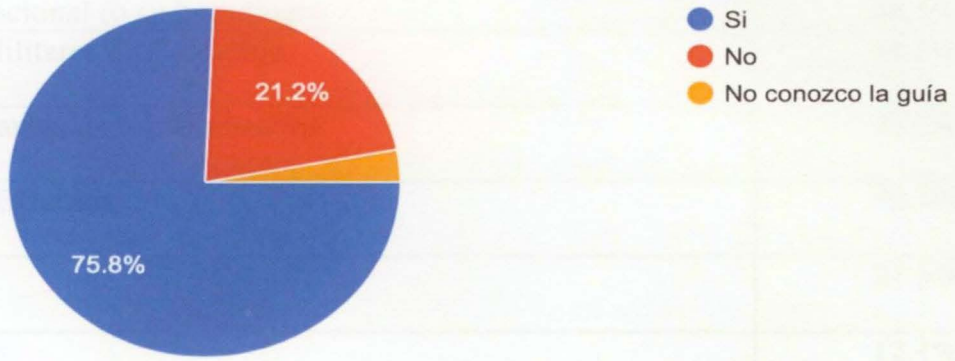
Figura 16. Porcentaje de experiencia de los encuestados en la administración de la ICC.



Fuente: Encuesta personal de expertos, (2020).

Con respecto a la pregunta: ¿Ha utilizado en su empresa u organización las directrices establecidas en la Guía para la ICC de Colombia que se desarrolló en el año 2015?; como se muestra en la figura 17, el 75.8% del personal participante en la mesa de trabajo manifiesta que sí ha utilizado las directrices, el 21.2% señala no haberla usado y un 3% no conoce la existencia de la Guía.

Figura 17. Conocimiento de la guía para la identificación de la ICCC.



Fuente: Encuesta personal de expertos, (2020).

De estas respuestas podemos analizar que a pesar de que la Guía Metodológica fue publicada en el año 2015, aproximadamente un 24% de las personas encuestadas no la emplean, lo cual evidencia la falta de desconocimiento, al igual que no les representa un elemento importante para la identificación de su ICC, lo cual también evidencia la necesidad de generar políticas que obliguen su utilización.

A la pregunta: ¿Quiénes deben participar en el proceso de identificación de ICC en Colombia?, los encuestados responden lo que se muestra en la tabla 10 y en la figura 18. Los expertos ven la necesidad de interacción entre el sector público, privado y la academia, durante el proceso de identificación de las ICCC.

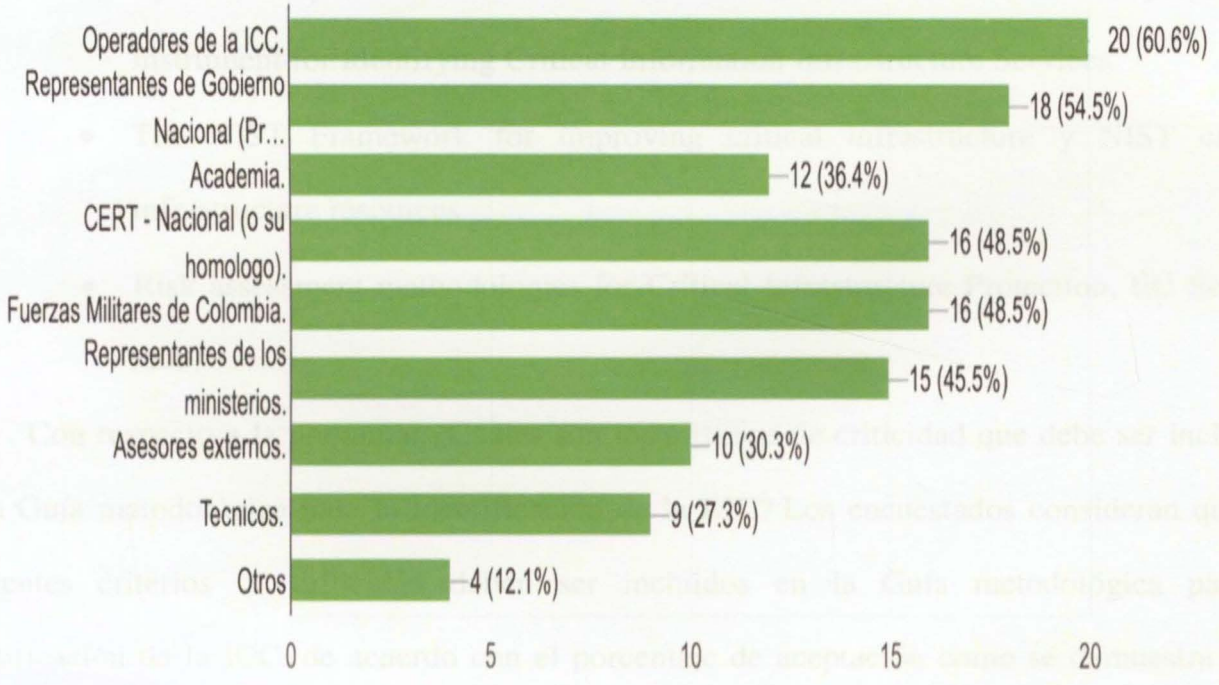
Tabla 10. Porcentaje de participación en la identificación de la ICCC.

Opción	**Porcentaje**
Operadores de las ICC.	60.6%
Representantes de Gobierno Nacional (Presidencia).	54.5%

Opción	Porcentaje
Academia	36.4%
CERT- Nacional (o su homólogo)	48.5%
Fuerzas Militares de Colombia	48.5%
Representantes de los Ministerios	45.5%
Asesores Externos	30.3%
Técnicos	27.3%
Otros	12.1%

Fuente: Elaboración propia, (2020).

Figura 18. Porcentaje de participación en la identificación de la ICCC.



Fuente: Encuesta personal de expertos, (2020).

Los encuestados recomiendan que los elementos o fases que deberían tener la Guía metodológica para la identificación de ICC en Colombia sean:

- Definir los principales actores que participarían en la identificación de la ICCC.
- Establecer unos criterios de criticidad, con el fin de identificar la priorización de cada servicio crítico a nivel nacional.
- Implementar metodología de manera continua y cíclica.

Con respecto a la pregunta: ¿Conoce usted alguna guía metodológica, política, procedimiento o estándar (nacional o internacional) que debería ser utilizado para la identificación de ICC en Colombia? El 24.2% manifiesta no conocer ningún documento o guía para la identificación de la ICCC, versus el 75.8%, quienes relacionan documentos, tales como:

- Guía para la Identificación, clasificación y catalogación de Infraestructura Crítica Cibernética (ICC) de Colombia. V 1.0
- Cybersecurity Officer - Colombian Air Force. Dirección de ... A Comprehensive Instrument for Identifying Critical Information Infrastructure Services.
- The NIST Framework for improving critical infrastructure y NIST critical infrastructure resources.
- Risk assessment methodologies for Critical Infrastructure Protection, EU Science Hub.

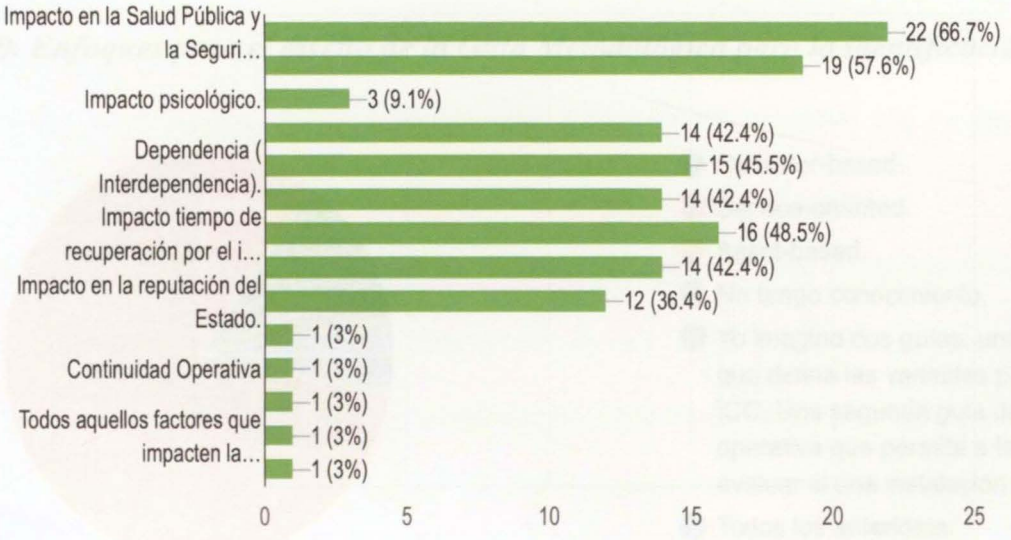
Con respecto a la pregunta: ¿Cuáles son los criterios de criticidad que debe ser incluidos en la Guía metodológica para la identificación de la ICC? Los encuestados consideran que los siguientes criterios de criticidad deben ser incluidos en la Guía metodológica para la identificación de la ICC, de acuerdo con el porcentaje de aceptación como se demuestra en la tabla 11 y en la figura 19.

Tabla 11. Criterios de criticidad en la Guía metodológica para la identificación de la ICC.

Opción de criterios	Porcentaje
Impacto en la salud pública y la seguridad nacional	66.7 %
Impacto económico	57.6 %
Impacto tiempo de recuperación	48.5 %
Dependencia (interdependencia)	45.5 %
Impacto medioambiental	42.4%
Impacto político	42.4 %
Impacto legal	42.4%

Fuente: Elaboración propia, (2020).

Figura 19. Criterios de Criticidad para la identificación de la ICCC.

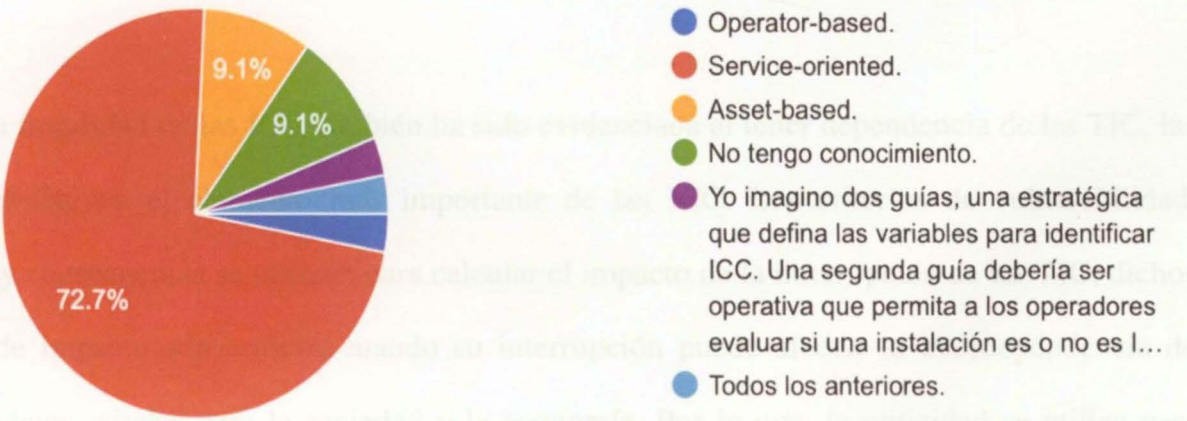


Fuente: Encuesta personal de expertos, (2020).

De las respuestas anteriores se puede analizar que los expertos ven criterios como la salud pública y la seguridad humana, dentro de la cual se enmarca la afectación a la población, una gran relevancia para llevar a cabo la identificación al obtener el porcentaje más alto con un 66%; el impacto económico sigue manteniendo una prevalencia sobre otros criterios y un factor como la dependencia que no se encuentra dentro de la guía anterior también es considerado por los expertos como importante; los expertos también consideran que la interconectividad entre las infraestructuras, al presentarse una falla en una de ellas, podría causar el colapso de las otras.

Las respuestas a la pregunta ¿Qué enfoque debería tener la Guía Metodológica para la identificación de ICC en Colombia? Permiten establecer que el 72.7% cree que el enfoque Service-oriented se ajusta a las características propias del País; el 9.1% señala el Asset-based; el 3% considera que el Operator-based es la metodología indicada; pero un 9.1% de los encuestados dicen no tener conocimiento de una metodología específica para la identificación de la ICC en Colombia.

Figura 20. Enfoques para el diseño de la Guía Metodológica para la identificación de ICCC.



Fuente: Encuesta personal de expertos, (2020).

Finalmente, la encuesta analizada permite determinar, como los expertos ven necesario que se encuentre involucrado en el proceso de identificación de las ICC, todos los sectores y diferentes actores del sector público y privado, que coadyuven de manera activa e integral, a una mejor priorización de los activos y posteriormente su protección eficaz y eficiente, de la mano de nuevos criterios propuestos, que busquen una mejor catalogación de las infraestructuras críticas, con el fin de direccionar de manera más asertiva los esfuerzos de la ciberdefensa a través del CCOCI, bajo la premisa de hacer menos vulnerables o más resistentes los sistemas vitales de los que todos dependemos, mediante la colaboración y cooperación de todos los actores, siendo esta la mejor defensa contra los riesgos y amenazas.

4.3 Criterios para la identificación, catalogación y priorización de la ICCC.

A través de la revisión documental y de las dos encuestas realizadas se ha ratificado la importancia de la identificación de las IC, ya que los servicios esenciales que estas soportan son vitales para las naciones. Este proceso de identificación se apoya a través de un número indefinido de criterios, los cuales son elementos de referencia sobre los cuales se toma una decisión

La fragilidad de las ICC también ha sido evidenciada al tener dependencia de las TIC, las cuales constituyen el elemento más importante de las ICC. Los criterios de vulnerabilidad, amenaza y consecuencia se utilizan para calcular el impacto de la interrupción de las TIC; dichos factores de impacto son críticos cuando su interrupción puede afectar la interdependencia de otros servicios, vitales para la sociedad y la economía. Por lo que, la criticidad se utiliza para evaluar el nivel de impacto de una interrupción de los servicios pertenecientes a la ICC, a través del uso de la combinación de dos influencias: (1) relevancia: se denota como el grado de pertinencia de un servicio vital para la supervivencia de un gran porcentaje de la sociedad; y,

(2)riesgo: se genera cuando el servicio se convierte en una amenaza a los otros servicios y factores, por ejemplo, el desabastecimiento de alimentos, fallas en las telecomunicaciones, entre otras. (Fekete, 2011, p.16).

Los criterios de criticidad a menudo se utilizan para establecer inventarios, registros de riesgos y prioridades de protección (Moteff, 2015).

Sin embargo, independientemente del enfoque o metodología a utilizar para la identificación, catalogación y priorización de la ICC de Colombia, se debe tener como referencia que en una infraestructura catalogada como crítica se debe evaluar el nivel de impacto con respecto a las amenazas relacionadas con la ciberseguridad (Theoharidou, Panayiotis Kotzanikolaou y Dimitris, 2009).

El impacto generalmente se evalúa con respecto a tres características principales:

- Distribución geográfica: el área que se impactaría por la interrupción inesperada de un servicio crítico.
- Magnitud: las consecuencias o efectos causados por la interrupción del servicio.
- Los efectos del tiempo: cuantificado en segundos, minutos, horas y/o días, en que un servicio considerado crítico tiene un impacto grave en otra infraestructura o en la sociedad. (Herrera L. C., 2019).

La distribución geográfica es el valor cuantitativo que se obtiene al evaluar cómo una proporción de la población puede verse afectada si un servicio vital es interrumpido por un programa malicioso o ataque cibernético.

La magnitud se establece utilizando criterios cuantitativos. La Comisión Europea establece un conjunto mínimo de criterios para que los Estados miembros incluyan en sus evaluaciones durante la priorización de los servicios críticos (Commission-European, 2006):

(a) efecto público, (b) efecto económico, (c) efecto ambiental, (d) interdependencia, (e) efectos políticos, (f) confianza en el gobierno y (g) efectos psicológicos.

Sobre la magnitud también el Plan Nacional de Protección de Infraestructura de EE. UU., lista los criterios para evaluarla las consecuencias: (a) salud pública y seguridad, (b) económico, (c) efecto psicológico y (d) gobernanza. (Dept. of Homeland Security, 2009)

Usando los datos recolectados mediante la encuesta aplicada a 33 expertos en el área y tomando como referente a los países miembros de la Unión Europea y los Estados Unidos, la siguiente tabla muestra criterios que son similares y podrían incluirse en una lista genérica de criterios de criticidad:

Tabla 12. Listado de Criterios para la identificación de la ICC.

Impacto	Unión Europea	EE. UU.	Colombia	Encuestados
Salud Pública y la Seguridad Nacional	X	X	X	X
Económico	X	X	X	X
Psicológico	X	X		
Político	X	X		X
Dependencia (Interdependencia)				X
Medioambiental	X		X	X
Legal				X
Reputación del Estado				X
Tiempo de recuperación del incidente				X

Fuente: Elaboración propia, (2020).

Aunque la Comisión Europea estableció sus criterios en el año 2006 y los Estados Unidos en el año 2009, en los últimos años han aparecido nuevos conceptos relacionados con la ICC, siendo la dependencia (interdependencia) uno de esos conceptos (intersectorial y transfronterizo).

Entonces, Las Infraectructuras Criticas están interconectadas y son mutuamente dependientes de una forma compleja, y la indisponibilidad repentina de cualquiera de ellas o parte de ellas puede causar la pérdida de vida, impacto severo en la salud, la seguridad o la economía (Taia, K., Kizhakkedatha A., Lin, J., Tiong, R. & Simc R.(2013), por lo cual la interdependencia es un criterio importante a ser tenido en cuenta en el proceso de identificación de las ICC.

Ahora bien, el aporte realizado por el personal de expertos, con experiencia y conocimiento en ICC, quienes mencionaron la relevancia en el proceso de identificación de la ICC en Colombia, para casos como el de salud pública; es respaldado en estudios como el de Fekete (2011), para quien muchas infraestructuras son importantes, pero solo cuando alcanzan cierto umbral crítico (tamaño, relevancia, o fragilidad); y una infraestructura revela su criticidad por el impacto negativo que causaría su destrucción o interrupción.

Con el fin de parametrizar la guía metodológica se requiere establecer unos criterios mínimos de criticidad; los siguientes criterios serán los propuestos como de mayor impacto para llevar a cabo el proceso de Identificación de las ICC en Colombia, como se ilustra en la figura 21, tomando como referencia a (ENISA, 2014), así:

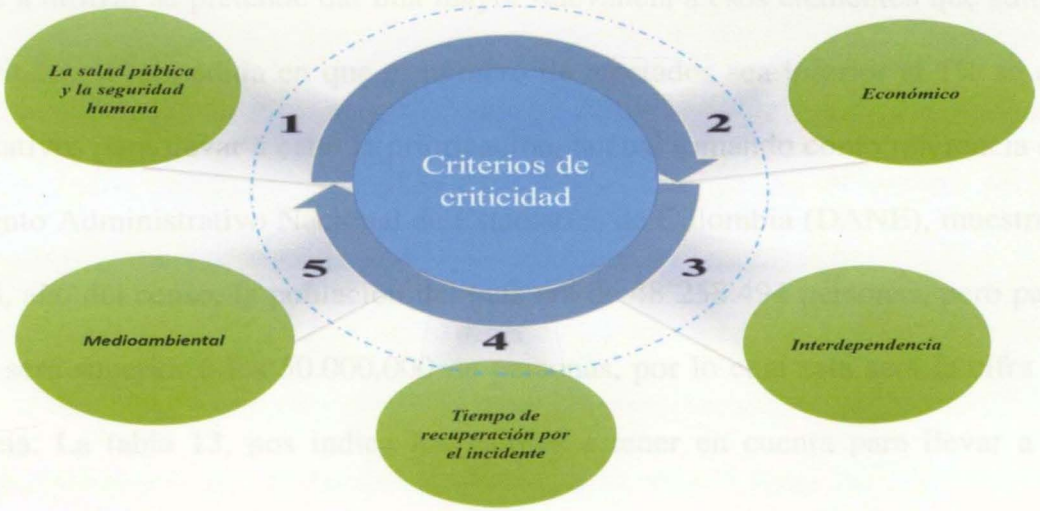
1. La salud pública y la seguridad humana: efecto sobre la vida humana y el bienestar físico.

2. Económico: efecto del PIB, importancia de la pérdida económica y / o degradación de productos o servicios.
3. Interdependencia: interdependencias entre elementos críticos de la infraestructura
4. Tiempo de recuperación por el incidente: el tiempo de indisponibilidad en que podría permanecer la infraestructura (inmediato, horas, uno o dos días, una semana).
5. Medioambiental: efecto sobre el público y el medio ambiente circundante.

Con estos criterios se busca llevar a cabo una mejor priorización de las ICCC, para reducir la vulnerabilidad por causas intencionales, mediante el empleo del ciberespacio.

La práctica permite determinar que identificar los activos criticos es un proceso sencillo; sin embargo, establecer la criticidad de un activo se hace complejo en comparación con los otros activos existentes (Izuakor, C. & White, R., (2017), por lo que se hace necesario establecer las escalas de cada uno de los criterios, empleando diversos modelos y metodologías, en los cuales se emplean medidas cualitativas (Bajo, Medio y Alto), al igual que medidas cuantitativas para obtener más precisión (Vogt, 2004).

Figura 21. Criterios de criticidad para la identificación de las ICCC.



Fuente: Elaboración propia, (2020).

4.3.1 Salud pública y seguridad humana.

El impacto sobre la salud pública y la seguridad humana, es el efecto producido por algún tipo de incidente sobre la vida humana y el bienestar físico, teniendo en cuenta que el impacto de este criterio, para el país y su población, representa una amenaza que conlleva al impedimento del logro del máximo potencial de desarrollo de individuos y comunidades y también el bienestar, la salud o incluso la vida de cientos de miles de personas afectados se pone en riesgo (Islas, 2019).

Con la inclusión de este criterio se proyecta proteger las libertades humanas esenciales; más aún si se tiene en cuenta la alta responsabilidad por parte de los gobiernos de salvaguardar a la población de los riesgos y amenazas que pueden perjudicar sus aspiraciones y su calidad de vida (Roses, 2012), es así como este criterio de impacto es importante para el proceso de identificación de las ICCC.

Para medir el impacto en este criterio, tomando los aportes realizados por expertos en las encuestas, el valor más alto será asignado, cuando la interrupción y no disponibilidad en un servicio esencial afecta a más del 1% de la población nacional en el territorio colombiano, con este porcentaje a utilizar se pretende dar una mayor relevancia a esos elementos que suministran los servicios vitales; a la medida en que el número de afectados sea inferior al 1% se asignará valores cuantitativos para llevar a cabo la priorización, la cual tomando como referencia el censo del Departamento Administrativo Nacional de Estadística de Colombia (DANE), muestra que en junio del 2018, año del censo, la población del país era de 48'258.494 personas, pero para junio del año 2020, será superior a los 50.000.000 de personas, por lo cual esta será la cifra a tomar como referencia. La tabla 13, nos indica los valores a tener en cuenta para llevar a cabo la priorización.

Tabla 13. Escala de impacto en la salud pública y seguridad humana.

Impacto	Cualitativo	Muy alto	Alto	Medio	Bajo
	Cuantitativo	7	5	3	1
Personas afectadas		500.000 o más. (Equivale al 1% de la población total)	250.000 a 499.000. (Equivale al 0,5% al 0,99%)	100.000 a 249.000 personas (Equivale al 0,499% al 0,2%)	Menos de 99.000 mil personas

Fuente: Elaboración propia, (2020).

4.3.2 Impacto Económico.

El impacto económico es el efecto que un ataque cibernético provoca sobre la economía de un Estado, ocasionando consecuencias negativas sobre su Producto Interno Bruto (PIB) y en el desarrollo económico de este. La economía resulta ser muy importante para un país por su capacidad para generar empleo y para dinamizar sectores o colectivos con especiales problemas de desarrollo económico (Fuentes & Mainar, 2015).

Con la inclusión de este criterio durante el proceso de identificación de las ICCC, se proyecta proteger la economía nacional, en donde su impacto negativo, genera consecuencias como reducción de la capacidad productiva, desvalorización de las empresas, pérdidas de empleos, entre otros, que pueden conllevar a la alteración del orden público.

Para medir el impacto en este criterio, tomando los aportes realizados por expertos en las encuestas, y de algunos de los enfoques mencionados en ENISA (2014), y la metodología desarrollada por la República Checa en su marco legal para la infraestructura crítica del año 2014, en donde el umbral asignado para determinar el impacto es del 0,5%, es

decir cuando la interrupción e indisponibilidad de una infraestructura que suministra un servicio esencial, afecte a la economía en un 0,5% o más con referencia al PIB de Colombia, a la infraestructura que genere este tipo de afectación en una escala cualitativa y cuantitativa se le asignará el puntaje superior, a la medida en la afectación económica sea inferior al 0,5% se asignará otros valores para llevar a cabo la priorización, la tabla 14, se indica los valores a tener en cuenta para llevar a cabo la priorización.

Tabla 14. Escala de Impacto económico.

Impacto	**Cualitativo**	**Muy alto**	**Alto**	**Medio**	**Bajo**
	Cuantitativo	**7**	**5**	**3**	**1**
Afectación sobre el Producto Interno Bruto (anual) del país.		(Del 0,5 % o más)	(Del 0,499% al 0,3%)	(Del 0,299 al 1%)	Inferior al 0,99%

Fuente: Elaboración propia, (2020).

4.3.3 Impacto de la Interdependencia de las infraestructuras.

Rinaldi (2004), argumentó que las infraestructuras críticas están altamente interconectadas y son dependientes mutuamente en una manera compleja, tanto física como a través de una serie de información y tecnologías de la información. Esta interdependencia complica aún más a las ICC, y gran parte de la nueva vulnerabilidad de estos sistemas se debe a las interdependencias cibernéticas, dependencias, que pueden provocar fallas en un sector y provocarlas en otro, un efecto cascada (Weggener, 2013), lo que incrementa el riesgo y las vulnerabilidades entre las infraestructuras de los diferentes sectores estratégicos.

Como las interdependencias demuestran que la interrupción, perturbación y/o destrucción de una IC tendría consecuencias catastróficas con impacto intersectorial e incluso internacional, con la inclusión de este criterio, durante el proceso de identificación de las ICCC, se espera

mitigar los efectos perjudiciales que conllevan los ciberataques para otros sistemas fundamentales y para los servicios que son críticos para la seguridad, prosperidad y bienestar social de una nación (Rinaldi, 2004).

Para medir el impacto en la interdependencia, se toman los aportes realizados por expertos en las encuestas y la selección de criterios para identificar infraestructuras críticas del Estado de Canadá, a traves del "marco de acción y para construir una resiliencia infraestructura crítica nacional". Este criterio proporciona una evaluación de posibles dependencias que otros servicios o funciones críticos puedan tener sobre el activo que se está revisando. El valor cuantitativo asignado en la escala de medición propuesta, sera el más alto, es decir, cuando la interrupción e indisponibilidad causada a una infraestructura crítica cibernética, genere la afectación sobre otras infraestructuras pertenecientes a 6 de los sectores del país, entre ellos 04 establecidos por el CCOCI como impacto muy alto, ellos son: electricidad, financiero, hidrocarburos y tecnologías de la información y comunicaciones, y 02 de impacto alto, ellos son: agua, seguridad y defensa, gobierno y transporte, como lo ilustra la figura No 22.

Figura 22. Escala de valoración impacto en los sectores estratégicos.

No.	SECTOR	IMPACTO CIBERNÉTICO
1	Alimentación y Agricultura	Bajo
2	Agua	Alto
3	Comercio, Industria y Turismo	Medio
4	Seguridad y Defensa	Alto
5	Educación	Moderado
6	Electricidad	Muy Alto
7	Financiero	Muy Alto
8	Gobierno	Alto
9	Recursos Naturales-medio Ambiente	Bajo
10	Recursos Minero Energéticos	Muy Alto
11	Salud y Protección Social	Moderado
12	Tecnologías de Información y Comunicaciones	Muy Alto
13	Transporte	Alto

Escala Valoración Impacto

Fuente: Ministerio de Defensa Nacional, (2016).

Con este porcentaje a utilizar se pretende dar una mayor relevancia a esos elementos que suministran los servicios vitales; a medida que el número de sectores afectados sea inferior al valor mayor proyectado, los valores cuantitativos serán menores, para llevar a cabo la priorización, como se indica en la Tabla 15.

Tabla 15. Escala de Impacto en la Interdependencia de las Infraestructuras.

Impacto	**Cualitativo**	**Muy alto**	**Alto**	**Medio**	**Bajo**
	Cuantitativo	**7**	**5**	**3**	**1**
Impacto a raíz de la interdependencia con otros sectores.		Al impactar los 4 sectores de impacto muy alto y 2 sectores de impacto alto.	Al impactar 3 sectores de impacto muy alto y 1 sector de impacto alto.	Al impactar 2 sectores de impacto muy alto y 1 sector de impacto alto.	Al impactar sector de impacto muy alto y 1 sector de impacto alto

Fuente: Elaboración propia, (2020).

4.3.4 Tiempo de recuperación de la infraestructura.

La disponibilidad de las ICC garantiza el buen funcionamiento de los diferentes sectores que suministran los servicios esenciales de la nación, por eso su indisponibilidad puede generar consecuencias devastadoras. El impacto del tiempo de recuperación de la infraestructura es el tiempo en el cual la ICC logra recuperar el servicio, desde el momento que se lleva a cabo la interrupción (Theoharidou, Panayiotis Kotzanikolaou, & Dimitris, 2009).

Con la inclusión de este criterio en el proceso de identificación de las ICCC, se pretende conocer de una u otra manera la capacidad que poseen las infraestructuras para responder a los problemas críticos en el corto plazo, de tal manera que la sociedad pueda funcionar de inmediato a los niveles que existían inmediatamente antes de la aparición del desastre (UNDP, 2018).

Para medir el impacto en este criterio, se usan los aportes realizados por (Herrera L. C., 2019) así: el valor cuantitativo y cualitativo asignado en la escala de impacto que se propone, será el más alto, cuando el tiempo de recuperación de la infraestructura con referencia a la interrupción e indisponibilidad causado por un ciberataque, corresponda a un tiempo entre 36 y 48 horas, a medida que el tiempo de recuperación vaya disminuyendo, de la misma manera será menor el valor cuantitativo y cualitativo asignado, con este porcentaje a utilizar se pretende dar una mayor relevancia a la priorización, al contar con más criterios para llevar a cabo la catalogación de las ICCC. En la tabla 16, se referencia los valores a tener en cuenta.

Tabla 16. Escala de Impacto del tiempo de recuperación de la infraestructura.

Impacto	**Cualitativo**	**Muy alto**	**Alto**	**Medio**	**Bajo**
	Cuantitativo	**7**	**5**	**3**	**1**
Impacto por el tiempo en que la infraestructura logra recuperar el servicio.		36 a 48 horas	24 a 36 horas	12 a 24 horas	0 a 12 horas

Fuente: Elaboración propia, (2020).

4.3.5 Medioambiente.

Debido al crecimiento de los problemas ambientales durante las últimas décadas, el medio ambiente ha cobrado amplio reconocimiento. Se considera un impacto ambiental la alteración, modificación o cambio en el ambiente, o en alguno de sus componentes de cierta magnitud y complejidad o producido por los efectos de la acción o actividad humana (Soriano, Ruiz & Ruiz, 2015).

Para medir el impacto en este criterio, se toma como referencia el valor empleado en la guía metodológica actual (CCOCI, 2015), es así como el valor cuantitativo y cualitativo más alto asignado en la escala de impacto que se propone, será el impacto ambiental por tres años o más como causa de la interrupción o afectación de una ICC, a medida que el tiempo de impacto

ambiental vaya disminuyendo, de la misma manera será menor el valor cuantitativo y cualitativo asignado, como se muestra en la tabla 17.

Tabla 17. Escala impacto ambiental.

Impacto	**Cualitativo**	**Muy alto**	**Alto**	**Medio**	**Bajo**
	Cuantitativo	**7**	**5**	**3**	**1**
Impacto en el medioambiente		3 años o más	2 años	1 año	0 a 11 meses

Fuente: Elaboración propia, (2020).

Ahora bien, al determinar de acuerdo a la escala de impacto la afectación que puede presentar una ICC en cada criterio, es pertinente determinar la importancia de los criterios propuestos, darle un peso, es decir la medida de la importancia relativa que el criterio tiene para la toma de decisiones (Muñoz & Romana, 2016). Para determinar el peso, se elaboró una encuesta[7], a través del CCOCI, con preguntas estructuradas para determinar a través de la experiencia de los encuestados, aportes que nos lleven a precisar el peso que debe ser asignado a cada uno de los criterios.

La población que fue tenida en cuenta para llevar a cabo la recolección de datos, pertenecen a los diferentes sectores estratégicos del Estado colombiano, quienes poseen conocimiento y experiencia en temas administrativos, operativos y académicos relacionados con las ICC; así mismo hacen parte de las diferentes reuniones de "Infraestructura Critica, Riesgo Operacional y Ciberdefensa" evento organizado por el Comando Conjunto Cibernético (CCOCI).

[7] https://docs.google.com/forms/d/1f-lbRcqyVf0cpdOqdO21b2K4ZsZFB0G_Tug9D7E3FCA/edit

La siguiente fue la consulta realizada en la encuesta, "teniendo en cuenta los criterios propuestos para llevar a cabo la identificación de las ICC de Colombia, califique de 1 a 10 la relevancia/peso de cada uno de los criterios, 10 significa que la variable es muy relevante y 1 poco relevante, se permiten calificaciones iguales entre criterios". En esta encuesta se obtuvo el aporte de 44 expertos[8], los cuales determinaron la importancia y/o relevancia de los criterios de acuerdo a la tabla 18.

Tabla 18. Orden de relevancia de los criterios de acuerdo a la encuesta a expertos.

Orden de relevancia	Criterio	Valor total obtenido en la encuesta (sobre 440)	Valor de relevancia
1	Tiempo de recuperación	398	9
2	Salud publica	394	8.95
3	Económico	393	8.93
4	Medioambiente	366	8.3
5	Interdependencia	364	8.2

Fuente: Elaboración propia, (2020).

Considerando los resultados de la encuesta, a cada criterio le fue otorgado un peso, con un valor de 1 a los 3 criterios que obtuvieron un valor de importancia cercano a 9 y un valor de 0,9 a los 2 criterios que obtuvieron un valor de importancia cercano a 8 como se muestra en la tabla 19.

Los valores fueron obtenidos a través del siguiente procedimiento:

Valor de importancia = Total de la calificación por criterio / total personal encuestado.

[8]https://docs.google.com/forms/d/1f-bRcqyVf0cpdOqdO21b2K4ZsZFB0G_Tug9D7E3FCA/edit#responses

Tabla 19. Relevancia y peso de los criterios propuestos.

Orden de relevancia	Criterio	Valor de importancia según los encuestados	Peso
1	Tiempo de recuperación	9	1
2	Salud publica	8.95	1
3	Económico	8.93	1
4	Medioambiente	8.3	0,9
5	Interdependencia	8.2	0,9

Fuente: Elaboración propia, (2020).

A continuación, tomando como base los resultados obtenidos, al determinar de acuerdo a la escala de impacto la afectación que puede presentar una ICC en cada criterio y el peso de cada criterio, se sumarán cada uno de los valores con el fin de llevar a cabo la priorización e identificación de las ICCC, como se representa en la tabla 20, en donde se muestra como la ICC A, tiene un mayor puntaje con respecto a la ICC B, lo cual le da una mayor relevancia y umbral crítico, para ser considera como una Infraestructura Critica Cibernética de Colombia, así:

Tabla 20. Matriz de criterios para la identificación de las ICCC.

Infraestructura A				**Infraestructura B**			
Criterio	**Valor escala Impacto**	**Peso**	**Valor Imp*P**	**Criterio**	**Valor Escala Impacto**	**Peso**	**Valor Imp*p**
Salud Pública	7	1	7	Salud Pública	3	1	3
Economía	5	1	5	Economía	3	1	3
Dependencia	7	0.9	6,3	Dependencia	3	0.9	2,7
Tiempo de recuperación	1	1	1	Tiempo de recuperación	3	1	3
Medio-ambiente	5	0.9	4,5	Medio-ambiente	1	0.9	0,9
Total	ICCC 23,8			12,6			

Fuente: Elaboración propia, (2020).

Para concluir, teniendo en cuenta que, entre más se usen los criterios de criticidad más preciso será el resultado, demostrando su criticidad al definirse como un tipo de importancia visible por los impactos negativos de una interrupción (Federal Ministry of the Interior of Germany, 2009), generarlos se convierten en una herramienta que permite la priorización y catalogación de las ICCC, todo esto con el objetivo último de determinar hacia dónde deben ser enfocado el esfuerzo de protección y defensa de las ICCC, para de esta manera preservar el bienestar de la población.

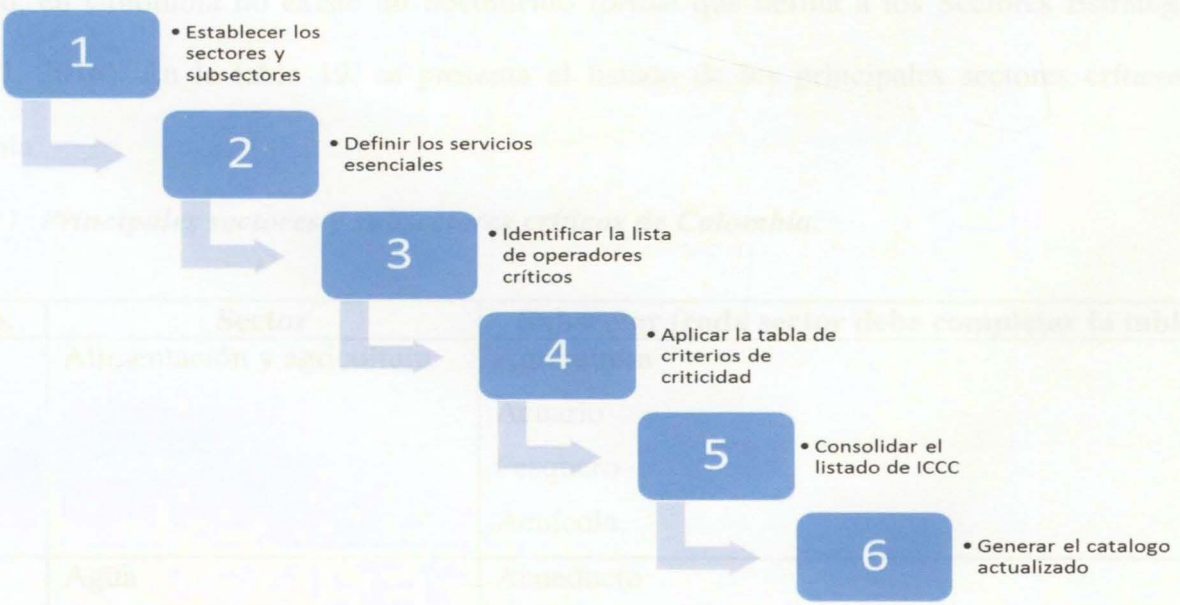
Lo que se busca a través del uso de los anteriores criterios es determinar la relevancia de una ICC e identificar cómo no se convierta en un riesgo y amenaza para la población. Es pertinente recordar lo expuesto por Fekete, (2011): aunque muchas infraestructuras son importantes, sólo cuando alcanzan cierto umbral crítico unas pasan a ser más importantes que otras.

Capítulo V

Propuesta de actualización de la guía metodológica para la identificación de ICCC.

En este capítulo, a partir de las encuestas y análisis realizados se propone y sugiere algunas líneas de trabajo que permitan llegar a la construcción de una segunda versión de la Guía Metodológica para la Identificación de las ICC de Colombia, la cual se estructuró a partir de la información recolectada de los expertos, de las políticas y metodologías ya existentes en el mundo; a través de la disposición de nuevos criterios, con escala de impacto, para guiar el proceso de identificación de la Infraestructura Crítica Cibernética en Colombia, bajo la coordinación de organismos tales como: el CCOCI y el ColCERT, como se ilustra en la figura 23.

Figura 23: Actividades para la identificación de las Infraestructuras Criticas Cibernéticas de Colombia.



Fuente: Elaboración propia, (2020).

La identificación de la ICCC podría realizarse a través de un instrumento que permita recolectar la información relevante de todos los servicios críticos. Además, se mencionan algunas actividades que no se han analizado en el presente trabajo, que deben ser desarrolladas para una eficaz identificación, tales como la capacitación del personal que opera la ICC para la recolección de información y el fortalecimiento en las capacidades del CCOCI y el ColCERT, desde donde se garantiza la continuidad de las mesas de trabajo para la identificación de la ICCC.

Acorde con las consideraciones anteriores, las principales actividades que se sugiere debe incluir la guía metodológica se describen a continuación.

Actividad No 1.

Establecer los sectores críticos a nivel nacional: en Colombia, en conjunto con el personal experto del gobierno, Fuerzas Militares, academia y empresas de los sectores públicos y privados, se han identificado 13 sectores nacionales, con sus respectivos subsectores; sin embargo, en Colombia no existe un documento formal que defina a los Sectores Estratégicos (CCOCI, 2016). En la tabla 19, se presenta el listado de los principales sectores críticos de Colombia.

Tabla 21. Principales sectores y subsectores críticos de Colombia.

Nro.	Sector	Subsector (cada sector debe completar la tabla)
1	Alimentación y agricultura	Agricultura Acuario Pesquero Acuícola
2	Agua	Acueducto Saneamiento básico Red matriz

Nro.	Sector	Subsector (cada sector debe completar la tabla)
3	Comercio, industria, turismo	Comercio Industria Turismo
4	Defensa	Unidad de Gestión General – MDN Ejército Nacional Armada Nacional Fuerza Aérea Colombiana Policía Nacional
5	Educación	Instituciones de Educación Preescolar, Básica, Media y Superior. Institutos para el Fomento de la Educación Superior. Entidades de Crédito Educativo. Entidades de Educación para personas con Discapacidad.
6	Electricidad	Operación Generación Transmisión Distribución Comercialización
7	Financiero	Intermediarios Financieros Portafolios de Inversión Aseguradores e Intermediarios de Seguros y Reaseguros Pensiones, Cesantías y Fiduciaria Intermediarios de Valores
8	Gobierno	Presidencia Políticas Públicas Planeación Nacional Hacienda Inteligencia

Nro.	Sector	Subsector (cada sector debe completar la tabla)
		Sistemas de emergencias Estadísticas Inclusión Social y Reconciliación
9	Recursos naturales-medio ambiente	Estratégico y Político Hidrológico, Meteorológico y Ambiental Parques Naturales y Áreas protegidas Licencias y Trámites Ambientales Conservación, Protección y Administración de los Recursos Naturales Renovables. Investigación Científica en Biodiversidad y Recursos Naturales.
10	Recursos minero-energéticos	Entidades adscritas Hidrocarburos Gas Minería Distribución
11	Salud y protección social	Salud pública Protección Social Vigilancia y supervisión.
12	Tecnologías de la información y comunicaciones	Tecnologías de la información Comunicaciones Tecnologías de Operación
13	Transportes	Terrestre Aéreo Marítimo y fluvial

Fuente: COCCI, (2016).

Actividad No 2.

Definir los servicios esenciales que suministra cada sector, de acuerdo a la definición CCOCI (2016); teniendo en cuenta que un servicio es esencial cuando es necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad o necesario para el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas. En la tabla 20, se relaciona un ejemplo de cómo se analizan los servicios esenciales, en función del sector y subsector al que pertenecen.

Tabla 22. Sector, subsector y servicios esenciales

Sector	Subsector	Servicio esencial	Justificación
Transporte	Marítimo y fluvial	Tráfico marítimo	Permitir el atraque y zarpe de cualquier tipo de buque para así dar continuidad al comercio exterior del país.

Fuente: Elaboracion propia, (2020).

Actividad No 3.

Identificar la lista de operadores potencialmente catalogados como críticos: El alcance es el valor que puede obtenerse evaluando cómo una proporción de la población puede verse afectada si un servicio sufre un ciberataque, según el análisis de tres factores propuestos por Fekete (2011) y Theoharidou M. (2009), (a) la concentración de la población afectada; (b) número de usuarios afectados; y, (c) impacto geográfico de la interrupción del servicio. La tabla 21, muestra el porcentaje propuesto de mapeo simple con los valores de criticidad.

Tabla 23. Porcentajes para identificar operadores y empresas potencialmente catalogadas como críticos.

Impacto	Muy alto	Alto	Medio	Bajo
Concentración de la población afectada por KM2	25.000 por 10 Km2 (tomando como referencia la densidad poblacional más alta de Colombia según estudio en la revista Journal of the American Planning Association)	25.000 por 100 km2	25.000 o más por 1000 Km2	25.000 o más por 10,000 km2
Impacto geográfico de la interrupción del servicio	Más de 1,000 km2	1,000 a 500 km2	100 a 500 km2	Menos de 100 km2

Fuente: Elaboración propia, (2020).

Actividad No 4.

Aplicar la tabla de criterios de criticidad a la infraestructura estratégica cibernética identificada en la actividad 3, considerando una afectación tal que impida la prestación del servicio por causa de la materialización de una amenaza cibernética. Los siguientes criterios son los propuestos como de mayor impacto para llevar a cabo el proceso de Identificación de las ICC en Colombia:

a) La salud pública y la seguridad: El efecto que causa este impacto sobre la vida humana y el bienestar físico.

b) Económico: El efecto sobre el PIB (anual), la importancia de la pérdida económica y / o degradación de productos o servicios.

c) Dependencia: El impacto a raiz de la interdependencia de una infraestructura sobre los demás sectores estratégicos.

d) Tiempo de recuperación por el incidente: El impacto del tiempo de recuperación de la infraestructura es el tiempo en el cual la ICC logra recuperar el servicio (inmediato, horas, uno o dos días, una semana).

e) Medioambiental: efecto que causa el impacto sobre el público y el medio ambiente circundante.

Las tablas 13, 14, 15, 16 y 17, muestran las escalas de impacto que se proponen para llevar a cabo la identificación de las ICCC, en cada uno de los criterios mencionados anteriormente, en donde cada una de las empresas u operadores tendrán como referencia los valores cualitativos y cuantitativos para establecer el valor del impacto de sus infraestructuras en caso de una interrupción.

Tabla 13. ***Escala de impacto en la salud pública y seguridad humana.***

Impacto	**Cualitativo**	**Muy alto**	**Alto**	**Medio**	**Bajo**
	Cuantitativo	**7**	**5**	**3**	**1**
Personas afectadas		500.000 o más. (Equivale al 1% de la población total)	250.000 a 499.000. (Equivale al 0,5% al 0,99%)	100.000 a 249.000 personas (Equivale al 0,499% al 0,2%)	Menos de 99.000 mil personas

Fuente: Elaboración propia, (2020).

Tabla 14. Escala de Impacto económico.

Impacto	Cualitativo	Muy alto	Alto	Medio	Bajo
	Cuantitativo	7	5	3	1
Afectación sobre el Producto Interno Bruto del país. (anual)		(Del 0,5 % o más)	(Del 0,499% al 0,3%)	(Del 0,299 al 1%)	Inferior al 0,99%

Fuente: Elaboración propia, (2020).

Tabla 15. Escala de Impacto en la Interdependencia de las Infraestructuras.

Impacto	Cualitativo	Muy alto	Alto	Medio	Bajo
	Cuantitativo	7	5	3	1
Impacto a raíz de la interdependencia con otros sectores.		Al impactar los 4 sectores de impacto muy alto y 2 sectores de impacto alto.	Al impactar 3 sectores de impacto muy alto y 1 sector de impacto alto.	Al impactar 2 sectores de impacto muy alto y 1 sector de impacto alto.	Al impactar sector de impacto muy alto y 1 sector de impacto alto

Fuente: Elaboración propia, (2020).

Tabla 16. Escala de Impacto del tiempo de recuperación de la infraestructura.

Impacto	Cualitativo	Muy alto	Alto	Medio	Bajo
	Cuantitativo	7	5	3	1
Impacto por el tiempo de recuperación de la infraestructura		36 a 48 horas	24 a 36 horas	12 a 24 horas	0 a 12 horas

Fuente: Elaboración propia, (2020).

Tabla 17. Escala impacto ambiental.

Impacto	Cualitativo	Muy alto	Alto	Medio	Bajo
	Cuantitativo	7	5	3	1
Impacto en el medioambiente		3 años o más	2 años	1 año	0 a 11 meses

Fuente: Elaboración propia, (2020).

Finalmente, al determinar la afectación que puede presentar una ICC, de acuerdo con la escala de impacto, en cada uno de los cinco criterios, datos que se suman, con el fin de establecer el valor que permita llevar a cabo la priorización e identificación de las ICCC prioritarias, Un ejemplo se presentó en la tabla 20.

Tabla 20. Matriz de criterios para la identificación de las ICCC.

Infraestructura A				Infraestructura B			
Criterio	**Valor escala Impacto**	**Peso**	**Valor Imp*P**	**Criterio**	**Valor Escala Impacto**	**Peso**	**Valor Imp*p**
Salud Pública	7	1	7	Salud Pública	3	1	3
Economía	5	1	5	Economía	3	1	3
Dependencia	7	0.9	6,3	Dependencia	3	0.9	2,7
Tiempo de recuperación	1	1	1	Tiempo de recuperación	3	1	3
Medio-ambiente	5	0.9	4,5	Medio-ambiente	2	0.9	1,8
Total	ICCC 23,8			13,5			

Fuente: Elaboración propia, (2020).

Ahora bien, según el valor total obtenido por la suma de los criterios, las empresas u operadores de la mano del CCOCI y el ColCERT, llevaran a cabo la identificación y priorización de las ICCC.

Actividad No 5.

Consolidar el listado de las Infraestructuras Críticas Cibernéticas de Colombia a través del CCOCI, con el fin de efectuar análisis que lleve a la priorización y catalogación, con base a la información suministrada por los sectores; en caso de dudas se debe solicitar a los sectores las respectivas aclaraciones sobre el proceso realizado.

Actividad No 6.

Generar un catálogo actualizado que permita al alto gobierno y a las agencias responsables de la identificación de ICCC asignar recursos para su protección. Este catálogo puede ser considerado una herramienta para la toma de decisiones y como punto de partida para establecer los posibles escenarios de crisis socioeconómica generados por la interrupción de un servicio vital.

A continuación, en la tabla 20, se presenta un resumen de las actividades propuestas para la identificación de la Infraestructura Crítica Cibernética de Colombia (ICCC), con los responsables de quienes depende que la aplicación de esta guía es el primer paso para proteger los servicios esenciales que son considerados críticos para Colombia.

Tabla 24. Lista de Actividades de la Guía Metodológica de ICCC.

No	Actividad	Responsable
1	Establecer los sectores críticos a nivel nacional.	Cada sector
2	Definir los servicios esenciales que suministra cada sector, de acuerdo con la definición (CCOCI, 2016)	Cada sector
3	Identificar la lista de operadores potencialmente catalogados como críticos a través del análisis de los siguientes factores:	Cada sector

No	Actividad	Responsable
	Número de usuarios afectados. Impacto geográfico de la interrupción del servicio.	
4	Aplicar la tabla de variables de criticidad a la infraestructura estratégica cibernética identificada en la actividad 3, bajo los siguientes criterios: 1. La salud pública y la seguridad. 2. Económico. 3. Dependencia. 4. Tiempo de recuperación por el incidente. 5. Medioambiental.	Cada sector
5	Análisis con base a la información suministrada por los sectores, que lleve a la priorización y catalogación de las ICCC	CCOCI
6	Generar un catálogo actualizado que permita al alto gobierno y a las agencias responsables de la identificación de ICCC asignar recursos para su protección.	CCOCI

Fuente: Elaboración propia, (2020).

Para concluir la identificación de la ICCC es un proceso que requiere y debe involucrar la participación de todos los sectores, donde la evaluación para la catalogación y priorización se basan principalmente en el impacto sobre los criterios de criticidad.

Es así como se establecieron los pasos mínimos necesarios para la identificación de la ICCC, estos se construyeron de acuerdo con la información académica, metodologías existentes, políticas y directrices oficiales, tales como: documentos CONPES y la guía metodológica para la

identificación de ICCC versión 1 del 2015, para este proceso de identificación se incluyen nuevos porcentajes y nuevos criterios para determinar la relevancia e importancia de una ICC con respecto a otra ICC, estos criterios son la interdependencia y el tiempo de recuperación, a raíz de la creciente necesidad del uso de las TIC para el buen funcionamiento de las infraestructuras Críticas y así mismo de la capacidad de estas de recuperar el servicio al momento de recibir un ciberataque que afecte su disponibilidad, confidencialidad e integridad.

Conclusiones.

En la presente monografía los objetivos diseñados fueron cumplidos en su totalidad, al usar conocimiento de expertos y revisión documental para la propuesta al Comando Conjunto Cibernético, de la actualización de la Guía para identificación de la Infraestructura Crítica Cibernética de Colombia (ICCC).

La revisión documental y la indagación mediante encuestas aportaron a la búsqueda del mejoramiento y fortalecimiento de procesos que permiten sugerir un modelo para identificar las ICC, y así prevenir posibles ataques o responder con efectividad, en caso de que se presenten; igualmente permitió precisar la urgencia del aporte de herramientas idóneas para su identificación, porque además de la importancia de identificar una IC, el hecho de incrementarse el uso de las TIC, las IC se convierten en ICC y que estás se concentran en diferentes sectores estratégicos para la nación, y que de ellas pueden depender otros sectores, de manera directa o indirecta.

Ahora bien, para el alcance del primer objetivo se realizó un análisis de las metodologías, lineamientos e información académica que involucra el proceso de identificación de la Infraestructura Crítica Cibernética de Colombia (ICCC). En donde se concluye, que la importancia de una IC se hace evidente y más visible en el momento que se presenta una falla, lo que lleva a lo no disponibilidad de manera imprevista de los servicios esenciales. Considerando que las IC a raíz de la búsqueda del mejoramiento y fortalecimiento de sus procesos funcionales han incrementado el uso de las TIC, convirtiendo a gran parte de las IC en ICC; es así como las TIC se constituyen en uno de los elementos más importantes de los servicios vitales de las ICC.

Hay que mencionar además, que todas estas ICC, se concentran en diferentes sectores estratégicos para la nación, a través de las cuales se garantizan la prestación de los servicios

esenciales, por lo cual su indisponibilidad amenaza la supervivencia o la viabilidad de estos sectores y al mismo tiempo de aquellos sectores que dependen de manera directa o indirecta de su disponibilidad, todo a raíz de la interdependencia informativa que se generan entre diferentes infraestructuras, por lo cual la vulnerabilidad de la ICC tienen un efecto significativo y hasta total en el funcionamiento de una infraestructura crítica, en donde su protección es determinante.

Por esta razón diferentes Estados y actores han desarrollado metodologías y enfoques para identificar, catalogar y priorizar las ICC, los cuales fueron analizados durante el desarrollo de la presente monografía, permitiendo recomendar unos elementos como criterios críticos, con los que se pretende llevar a cabo de manera más precisa y rigurosa el inventario de activos hacia los cuales se debe direccionar los esfuerzos y presupuestos para su protección. Todo esto en búsqueda de garantizar la funcionalidad, continuidad e integridad de las Infraestructuras Críticas Cibernéticas y de esta manera prevenir, debilitar y neutralizar una amenaza, riesgo o vulnerabilidad, para finalmente diseñar las pertinentes estrategias de mitigación y poder monitorear el estado operativo de las infraestructuras.

Para el alcance del segundo objetivo, se aplicó una herramienta para la recolección de datos primarios a personal experto en la gestión de la ICCC, con el objetivo de identificar las características, factores o variables de las Infraestructuras Críticas Cibernéticas. A través de las encuestas realizadas permitió determinar, como los expertos ven necesario, la actualización de la guía metodológica para la identificación de las ICCC del año 2015, de la mano de nuevos criterios propuestos, confirmados a través de encuestas a expertos, con los cuales se busca evaluar el nivel de impacto de una interrupción de los servicios esenciales pertenecientes a las ICC, los criterios de criticidad a menudo se utilizan para establecer inventarios, registros de riesgos y prioridades de protección (Moteff, 2015).

Con el fin de parametrizar la guía metodológica se sugiere el empleo de los siguientes criterios para llevar a cabo el proceso de Identificación de las ICC en Colombia, estos son, (1) la salud pública y la seguridad, (2) económico, (3) dependencia, (4) tiempo de recuperación por el incidente y (5) medioambiental. A través de estos criterios se busca llevar a cabo una mejor priorización de las ICCC, aportando elementos al Comando Conjunto Cibernético, para una segunda versión, a partir de la publicada en el 2015.

Para el alcance del tercer objetivo, se sugieren los pasos mínimos necesarios para la identificación de la ICCC, estos se proponen de acuerdo con la información académica, metodologías existentes, políticas y directrices oficiales, tales como: documentos CONPES y la guía metodológica para la identificación de ICCC versión 1 del 2015.

La identificación de la ICCC es un proceso que involucra la participación de todos los sectores, donde la evaluación para la catalogación y priorización se basan principalmente en factores de impacto de criticidad. Estos procesos involucran el análisis de riesgo, la conexión e interdependencia entre servicios esenciales, en los cuales la posible interrupción en uno de ellos podría generar un efecto en cascada y con esto el colapso de todos los servicios que son ofrecidos a una sociedad. Las seis actividades que se sugieren, son consideradas necesarias para el proceso de identificación de la ICCC; y aportan en el diseño de una segunda versión de la guía metodológica para la identificación de ICCC, cuya primera versión se publicó en el 2015.

Recomendaciones.

De acuerdo con la investigación realizada, la cual llevo a generar una propuesta que pueda ser tenida en cuenta para llevar a cabo el proceso de identificación y priorización de las ICC, se recomienda aplicar el instrumento de encuestas a base poblacional con experiencia en ICC, que permita hacer inferencias definitivas para el ejercicio.

Por otra parte, llevar a cabo una validación del modelo propuesto a través de un juicio de expertos con una metodología DELPHI, con el objeto de generar un consenso, que permita dar valor a la metodología propuesta.

Involucrar en el proceso de diseño de una nueva guía para la identificación de las ICC a todos los sectores y diferentes actores del sector público y privado, que coadyuven de manera activa en integral en una mejor priorización de los activos y posteriormente su protección eficaz y eficiente.

Referencias.

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Sistemas Asociación Colombiana de Ingenieros de Sistemas. 119, 4-7.

CCI. (2013). La proteccion de infraestructuras críticas y la ciberseguridad industrial. Madrid: CCI-ES.

CCOCI. (2015). Guía Metodológica para la identificación de Infraestructuras Críticas Cibernética de Colombia

CCOCI. (2016). Sectores estratégicos de la República de Colombia desde la óptica Cibernética.

Christensen, Caelli, Duncan & (2010) An Achilles heel: denial of service attacks on Australian critical information infrastructures, Information & Communications Technology Law, 19:1, 61-85, DOI: 10.1080/13600831003708059

Commission-European. (2006). Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection. Brussels: COM (2006)786 Final.

Dept. of Homeland Security. (2009). National Infrastructure Protection Plan.

Departamento Nacional de Planeacion. (2011). Lineamientos De Política para Ciberseguridad y Ciberdefensa. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Diario Oficial de la Unión Europea . (2016). Directiva (ue) 2016/1148 del parlamento europeo y del consejo. Obtenido de https://www.boe.es/doue/2016/194/L00001-00030.pdf

Dinero. (05 de Abril de 2018). Así está Colombia conectada a internet. Obtenido de https://www.dinero.com/pais/artículo/conectividad-de-colombia-a-internet-en-abril-de-2018/258047

DNP. (2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3701 https://www.mintic.gov.co/portal/inicio/3510:Conpes-3701-de-2011

ENISA. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

Erokhin, S., Petukhov, A., & Pilyugin, P. (2019). Critical Information Infrastructures Security Modeling. Proceeding Of The 24th Conference Of Fruct Association. https://dl.acm.org/doi/pdf/10.5555/3338290.3338302

Federal Office of Civil Protection and Disaster Assistance (BBK). (2017). Protecting Critical Infrastructures a Seven Step Identification Procces. https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/ProtectingCriticalInfrastructures.pdf?__blob=publicationFile

Fekete, A. (2011). Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science. https://doi.org/10.1007/s13753-011-0002-y

Frett, Nahum. (2015). ¿ Qué es un ciberataque?. https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque

Fuentes, P., & Mainar, A. (2015). Impacto económico y en el empleo de la Economía Social en España. Un análisis multisectorial. Revista De Economía Pública, Social y Cooperativa. https://www.redalyc.org/pdf/174/17440036004.pdf

Garcia Zaballos & Inkyung Jeun (2016). Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries. https://publications.iadb.org/publications/english/document/Best-Practices-for-

Critical-Information-Infrastructure-Protection-(CIIP)-Experiences-from-Latin-America-and-the-Caribbean-and-Selected-Countries.pdf

Gartner IT Glossary. (2015, August 15). Operational technology . Retrieved from http://www.gartner.com/it-glossary/operational-technology-ot .

GFCE. (2017). Critical information Infrastructure Protection. Global Forum on Cyber Expertise. https://thegfce.org/initiatives/critical-information-infrastructure-protection-initiative/

Gobierno de Chile. (2017). Política Nacional de Ciberseguridad. https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-ES-FEA.pdf

Gómez, E. (11 de Febrero de 2018). Identificación y Caracterización de Infraestructuras Críticas en Panamá. Actas de la conferencia. https://knepublishing.com/index.php/KnE-Engineering/article/view/1451/3506

Hahn A. (2016) Operational Technology and Information Technology in Industrial Control Systems. In: Colbert E., Kott A. (eds) Cyber-security of SCADA and Other Industrial Control Systems. Advances in Information Security, vol 66. Springer, Cham. https://doi.org/10.1007/978-3-319-32125-7_4

Harasta, J. (2018). Legally critical: Defining critical infrastructure in an interconnected world. International Journal of Critical Infrastructure Protection. https://www.researchgate.net/publication/325691427_Legally_critical_Defining_critical_infrastructure_in_an_interconnected_world

Herrera, L. C., & Maennel, O. (2019). A comprehensive instrument for identifying critical information infrastructure services. International Journal of Critical Infrastructure Protection, 25, 50-61

Hruza, P. (2018). Resiliencia y protección de la infraestructura de información crítica Resiliencia y protección de la infraestructura de información crítica. Comunicaciones - Cartas científicas de la Universidad de Zilina , 20 (2), 110-114 http://komunikacie.uniza.sk/index.php/communications/article/view/97

Hurtado, J. (2012). El proyecto de investigaciòn. Comprensiòn Holistica de la Metodología de la Investigación.Septima Edicion. Caracas: Quiron-ediciones.

Instituto de Auditores Internos de España. (Octubre de 2016). Buenas Prácticas en Gestión de Riesgos. Ciberseguridad Una guía de supervisión. https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

Islas ColínA., & Pérez BaxinO. (2019). Los conflictos y la vida diaria. Pensamiento Americano. https://doi.org/10.21803/pensam.v12i22.254.

Izuakor, CHristine. & White, Richard., (2017). Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis. 10th International Conference on Critical Infrastructure Protection (ICCIP), Mar 2016, Arlington, VA, United States. pp.27-41,

Li, Z. a. (2017). Cybersecurity in distributed power systems. Proceedings of the IEEE.

Liang, G., Weller, SR, Zhao, J., Luo, F. y Dong, ZY (2016). El apagón de Ucrania en 2015: implicaciones para los ataques de inyección de datos falsos. IEEE Transactions on Power Systems , 32 (4), 3317-3318.

Lietuvos Respublikos Vyriausybe. (2016). Nutarimas del Ypatingos Svarbos Informacines Infrastrukturo Sidentifikavimo Metodikos Patvirtinimo. Vilnius. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/77d6b4914f2611e68f45bcf65e0a17ee?jfwid=q8i88m9wc

Mahan, T & Menold, J (2020). Simulating cyber-physical systems: Identifying vulnerabilities for design and manufacturing through simulated additive manufacturing environments, Additive Manufacturing, Volume 35, October 2020, Article number 101232

Mattioli, R. a.-B. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. ENISA Report.

Mendez, A.(2018). Estudios de Metodologías de Ingenieria Social. Universitat Oberta de Catalunya.Http://openaccess.uoc.edu/webapps/o2/bitstream/10609/90305/6/amendezcarTFM12189memoria.pdf

Miller, B. a. (2012). A survey SCADA of and critical infrastructure incidents. Proceedings of the 1st Annual conference on Research in information technology. https://doi.org/10.1145/2380790.2380805

Mintzberg, H., & Lampel, J. (2005). Strategy bites back: It is a lot more, and less, than you ever imagined. Pearson Education.

Moteff, J. (2015). Critical infrastructures: Background, policy, and implementation. Congressional Research Service.

Muñoz, B, & Romana, M. (2016). Aplicación de metodos de decisión multicriterio discretos al anàlisis de alternativas en estudios de infraestructuras de transporte.

Nance, R., & Arthur, J. (1988). The methodology roles in the realization of a model development enviroment. Proceedings of the1988 winter simulation conference.

North Atlantic Treaty Organization (2014). Centre of excellence defence against terrorism. Critical infrastructure protection against terrorist attacks. Disponible en: http://www.coedat.nato.int/publication/course_reports/12-CIP.pdf

NITS. (2018). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

OECD. (2008). OECD Recommendation of the Council on OECD Legal Instruments the Protection of Critical Information Infrastructures https://legalinstruments.oecd.org/public/doc/121/121.en.pdf

Parlamento Europeo y Consejo de la Unión Europea (2016). Directiva (ue) 2016/1148 Diario Oficial de la Unión Europea https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=NL

Pescaroli, G., Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. Nat Hazards 82, 175–192 (2016). https://doi.org/10.1007/s11069-016-2186-3

Pipyros, K. a. (2018). A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. Computers & Security. https://doi.org/10.1016/j.cose.2017.04.007

Real Academia de la Lengua Española. (24 de julio de 2020). Real Academia Española. Obtenido de https://dle.rae.es/infraestructura?m=form

Rinaldi. (2004). Identifying, understanding, and analyzing critical infrastructure interdependencies. Proceedings of the 37th Hawaii International Conference on System Sciences. Hawaii: IEEE control systems magazine.

Robles, M. T. (2017). Guía Metodológica. Qué es? Cómo se realiza? https://docplayer.es/38155519-Guia-metodologica-que-es-como-se-realiza-1-definicion-de-objetivo-alcance-y-audiencia-aprobacion-difusion-edicion-y-diseno.html

Rodriguez, Maria. (2019). La protecciòn de infraestructuras críticas como un aspecto de la seguridad integral del Estado. Revista Estrategia, Centro de Altos Estudios Nacionales de Uruguay. https://www.gub.uy/ministerio-defensa-nacional/sites/ministerio-defensa-nacional/files/2020-03/Revista_Estrategia_6.pdf#page=9

Roses, M. (2012). Seguridad humana. Revista Panamericana de Salud Pública/Pan American Journal of Public Health, 351-354.

Sans. (2016). ICS Defense Use Case No. 6: Modular ICS Malware: Analysis of the Cyber Attack on the Ukrainian Power Grid. E-ISAC https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

Sharma, M. (2017). Securing Critical Information Infrastructures (Monografía) Institute for Defence Studies and Analyses, New Delhi. https://idsa.in/system/files/monograph/monograph60.pdf

Soriano, L., Ruiz, M. & Ruiz, E. (2015). Soriano Parra, Lady; Ruiz Rivera, María Elena; Ruiz Lizama, Edgar Criterios de evaluación de impacto ambiental en el sector minero Industrial Data, vol. 18, núm. 2, julio-diciembre, 2015, pp. 99-112 Universidad Nacional Mayor de San Marcos Lima, Perú.

Stouffer, K., Falco, J., & Scarfone, K. (2013). Guide to Industrial Control Systems (ICS) Security. United States of America Departement of commerce. http://dx.doi.org/10.6028/NIST.SP.800-82r1

Tabansky, L. (2011). Critical Infrastructure Protection against cyber threats. Military and Strategic Affairs, 3(2), 2. https://i-hls.com/wp-content/uploads/2013/03/Critical-Infrastructure-Protection-against-Cyber-Threats-Lior.pdf

Taia, K., Kizhakkedatha A., Lin, J., Tiong, R. & Simc R.(2013). Identifying Extreme Risks in Critical Infrastructure Interdependencies. International Symposium for Next Generation Infrastructure October 1-4, 2013, Wollongong, Australia.

Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering.

Theoharidou, M., Kotzanikolaou, P., & Gritzalis, D. (2009). Risk-based criticality analysis. In International Conference on Critical Infrastructure Protection Springer, Berlin, Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-642-04798-5_3.pdf

Tsochev, R., Yoshinov, D., & Iliev, O. (2019). Key problems of the critical information infrastructure through SCADA systems research. Academia de Ciencias de Bulgaria. DOI: 10.15622 / sp.2019.18.6.1333-1356

U.S. Goverment Accountability Office. (2013). Critical Infraestructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported. https://www.gao.gov/assets/660/653300.pdf

UNDP. (2018). Documento de Apoyo Infraestructura. Introducción a la Recuperación de la Infraestura. Capitulo I. Internacional Recovery Platform https://eird.org/pr14/cd/documentos/espanol/Publicacionesrelevantes/Recuperacion/6-Infraestructura.pdf

USA, C. (2001). Patriot act. Washington.

Vakulyk, O. & Petrenko, P., (2020). Cybersecurity as a component of the national security of the state. Journal of Security and Sustainability Issues, Volume 9, Issue 3, 2020, Pages 775-784

Valencia, A; Patiño, O & Garces, L., (2020). Research trends in the study of cyber defense: A bibliometric analysis. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao. Volume 2020, Issue E29, May 2020, Pages 366-379

Villalba, A. (2015). La ciberseguridad en España 2011–2015 una propuesta de modelo de organización (Tesis Doctoral) Universidad Nacional de Educación a Distancia (España) http://e-spacio.uned.es/fez/view/tesisuned:CiencPolSoc-Avillalba

Vogt, J. A. (2004). Chapter 4, Prioritizing Capital Projects. En J. A. Vogt, Capital Budgeting and Finance: A Guide for Local Governments. (págs. 89-118). ICMA.

Wegener, H., (2013). Los riesgos economicos de la ciberguerr. Cuadernos de estrategia, ISSN 1697-6924, Nº. 162, 2013 (Ejemplar dedicado a: La inteligencia económica de un mundo globalizado), págs. 177-227

Anexos.

Anexo 1. Primera encuesta a expertos en ICC

General

*Obligatorio

¿Cuál es el Sector Estratégico de su organización? *

- ◯ Agropecuario y Desarrollo Rural
- ◯ Agua
- ◯ Comercio, Industria y Turismo
- ◯ Seguridad y Defensa
- ◯ Educación
- ◯ Eléctrico
- ◯ Financiero
- ◯ Gobierno
- ◯ Recursos Naturales –Medio Ambiente
- ◯ Recursos Minero Energéticos
- ◯ Salud
- ◯ Tecnologías de la Información y las Comunicaciones
- ◯ Transporte
- ◯ Otro:

¿Considera necesaria la actualización de la Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia desarrollada en el 2015? *

- ◯ SÍ
- ◯ NO

¿Considera que los tres criterios de criticidad horizontal planteados en la guía requieren alguna modificación o ser eliminados? *

- ◯ SÍ
- ◯ NO

Anexo 2. Segunda encuesta a expertos en ICC

ACTUALIZACIÓN GUÍA METODOLÓGICA PARA LA IDENTIFICACIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS CIBERNÉTICAS DE COLOMBIA.

El objetivo principal de este cuestionario es recopilar información que permita diseñar una guía metodológica para la identificación de la Infraestructura Crítica Cibernética de Colombia.

Email address *

Valid email address

This form is collecting email addresses. Change settings

¿Cuál es su experiencia en la operación y/o administración de las ICC? *

- 0 a 5 años
- 5 a 10 años
- 10 a 15 años
- Mayor a 15 años

¿Ha utilizado en su empresa u organización las directrices establecidas en la Guía para la ICC de Colombia que se desarrolló en el año 2015? *

1. Si
2. No
3. No conozco la guía

¿Cuál es su ocupación actual? *

- Directivo
- Asesor
- Operario
- Experto en ICC

¿Cómo deberían ser definidas las Infraestructuras Críticas Cibernéticas (ICC) en Colombia)? *

Long answer text

¿Qué elementos o fases debería tener la Guía metodológica para la identificación de ICC en Colombia?

Long answer text

¿Conoce usted alguna guía metodológica, política, procedimiento o estándar (nacional o internacional) que debería ser utilizado para la identificación de ICC en Colombia? *

Long answer text

¿Qué enfoque debería tener la Guía Metodológica para la identificación de ICC en Colombia?

- Operator-based.
- Service-oriented.
- Asset-based.
- No tengo conocimiento.
- Other...

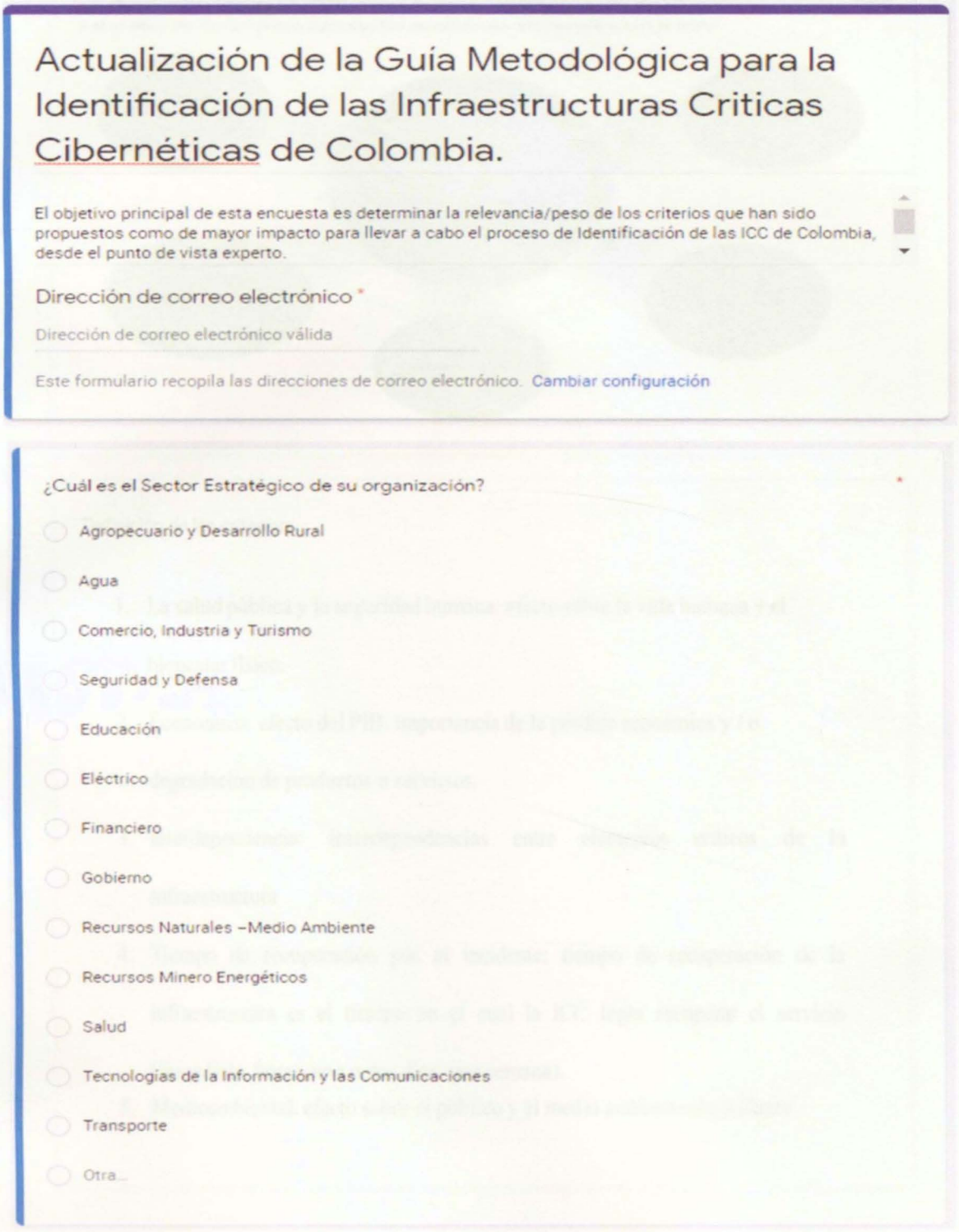
¿Quiénes deben participar en el proceso de identificación de ICC en Colombia ? *

- [ ] Operadores de la ICC.
- [ ] Representantes de Gobierno Nacional (Presidencia).
- [ ] Academia.
- [ ] CERT - Nacional (o su homologo).
- [ ] Fuerzas Militares de Colombia.
- [ ] Representantes de los ministerios.
- [ ] Asesores externos.
- [ ] Tecnicos.
- [ ] Otros

¿Cuáles son los criterios de criticidad que debe ser incluidos en la Guía metodológica para la identificación de la ICC? (Teniendo en cuenta los resultados de la primera encuesta realizada el 24 de septiembre de 2019, en el marco de LXVII reunión de infraestructura critica del Comando Conjunto Cibernetico y la lista genérica generada en común acuerdo entre la Unión Europea y EEUU) *

- [ ] Impacto en la Salud Pública y la Seguridad Nacional.
- [ ] Impacto económico.
- [ ] Impacto psicológico.
- [ ] Impacto Político (capacidad de Gobernar).
- [ ] Dependencia (Interdependencia).
- [ ] Impacto Medioambiental (Propuesto en la Guía del 2015).
- [ ] Impacto tiempo de recuperación por el incidente.
- [ ] Impacto legal.
- [ ] Impacto en la reputación del Estado.
- [ ] Other...

Anexo 3. Tercera encuesta a expertos en ICC.



Actualización de la Guía Metodológica para la Identificación de las Infraestructuras Criticas Cibernéticas de Colombia.

El objetivo principal de esta encuesta es determinar la relevancia/peso de los criterios que han sido propuestos como de mayor impacto para llevar a cabo el proceso de Identificación de las ICC de Colombia, desde el punto de vista experto.

Dirección de correo electrónico *

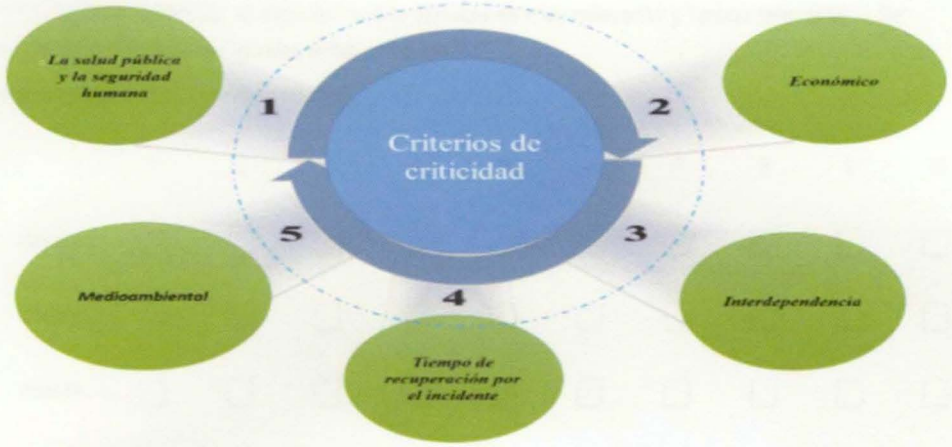
Dirección de correo electrónico válida

Este formulario recopila las direcciones de correo electrónico. Cambiar configuración

¿Cuál es el Sector Estratégico de su organización? *

- Agropecuario y Desarrollo Rural
- Agua
- Comercio, Industria y Turismo
- Seguridad y Defensa
- Educación
- Eléctrico
- Financiero
- Gobierno
- Recursos Naturales –Medio Ambiente
- Recursos Minero Energéticos
- Salud
- Tecnologías de la Información y las Comunicaciones
- Transporte
- Otra...

Los siguientes son los Criterios de Criticidad identificados como de mayor impacto y propuestos para la identificación de las ICCC, teniendo en cuenta la percepción de diferentes expertos en ICCC, y el análisis de documentos y productos académicos relacionados con el tema.



Definición de los criterios:

1. La salud pública y la seguridad humana: efecto sobre la vida humana y el bienestar físico.
2. Económico: efecto del PIB, importancia de la pérdida económica y / o degradación de productos o servicios.
3. Interdependencia: interdependencias entre elementos críticos de la infraestructura
4. Tiempo de recuperación por el incidente: tiempo de recuperación de la infraestructura es el tiempo en el cual la ICC logra recuperar el servicio (inmediato, horas, uno o dos días, una semana).
5. Medioambiental: efecto sobre el público y el medio ambiente circundante

Teniendo en cuenta los criterios propuestos para llevar a cabo la identificación de las ICC de Colombia, califique de 1 a 10 la relevancia/peso de cada uno de los criterios.
****OBSERVACIONESS: 10 significa que la variable es muy relevante y 1 poco relevante -- Se permiten calificaciones iguales entre criterios.****

*

Relevancia o peso de los criterios de criticidad.

	1	2	3	4	5	6	7	8	9	10
Salud p...	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Econó...	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Interde...	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Tiemp...	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Media...	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐