TIC

Lineamiento para la identificación de las infraestructuras críticas cibernéticas

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información
GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Lineamiento para la identificación de las infraestructuras críticas cibernéticas Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Tabla de Contenido

Tabla de Contenido 3
Listado de Tablas 3
Tabla de ilustraciones 4
Lineamientos en ciberseguridad 4
1. Marco Legal y Político 4
2. Instituciones Clave 5
3. La ciberseguridad para todos 5
Lineamiento para la identificación de las infraestructuras críticas cibernéticas 6
Resumen ejecutivo 6
Introducción 6
4. Normativa 7
5. Normativa Internacional 8
6. Algunos sectores y subsectores con alta criticidad 10
7. Antecedentes de las Infraestructuras Críticas y su metodología en Colombia 11
8. Roles y responsabilidades con la Ciberseguridad y Ciberdefensa de la infraestructura crítica cibernética: 13
9. Sectores Críticos Nacionales 2024 17
10. Amenazas y Riesgos a la infraestructura crítica digital 19
11. Derechos comprometidos por las ICC. 21
12. Casos comparados: Metodología Infraestructura Crítica Cibernética 22
13. Metodología para identificación de ICC en Colombia 25
14. Definición de las variables y explicación en la metodología: 32
15. Actualización en la metodología: 39
16. Orientación 40
17. Fuentes 48
18. ANEXOS: 49

Listado de Tablas

Tabla 21 Sectores y sus responsables 14

Tabla de ilustraciones

Ilustración 21 Comparativo de metodología de ICC internacional 25
Ilustración 22 Interdependencia de Infraestructura Crítica Cibernética de Estados Unidos 26
Ilustración 23 Interdependencia de infraestructura Crítica Cibernética de Colombia 27
Ilustración 24 Paso 3 identificación de ICC 38

Lineamientos en ciberseguridad

El contexto de ciberseguridad en Colombia y el mundo ha evolucionado significativamente en los últimos años, impulsado por el aumento de los riesgos y amenazas cibernéticas, el crecimiento de la digitalización y la necesidad de proteger tanto la infraestructura crítica como los datos personales de los ciudadanos. El país enfrenta diversos desafíos en el ámbito de la ciberseguridad, pero también ha logrado avances importantes en términos de políticas, legislación y cooperación internacional.

1. Marco Legal y Político

Colombia ha avanzado en la creación de un marco normativo y de políticas públicas para abordar los riesgos cibernéticos. Algunas de las iniciativas clave incluyen:

- **Ley 1273 de 2009:** Esta ley establece disposiciones para la protección de la información y la prevención de delitos informáticos, incluyendo fraudes electrónicos, acceso no autorizado a sistemas informáticos y otros crímenes cibernéticos. Aunque la ley es un paso inicial importante, su implementación y actualización se han visto desafiadas por la rapidez con la que evolucionan las amenazas.

- **Ley 1581 de 2012:** Esta ley regula la protección de datos personales en Colombia, estableciendo principios y derechos para la protección de la información personal de los ciudadanos. La Ley 1581 también se complementa con la creación de la Superintendencia de Industria y Comercio (SIC), que supervisa y garantiza el cumplimiento de la normativa en esta área.

- **Política Nacional de Seguridad Digital:** En el CONPES 3854 de 2016, busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.

- **Política Nacional De Confianza Y Seguridad Digital:** En el CONPES 3995 de 2020, establece una estrategia integral para proteger las infraestructuras críticas y mejorar la resiliencia del Estado frente a los riesgos cibernéticos. Este documento orienta la creación de políticas, normativas y mecanismos de protección para los sistemas e información más relevantes a nivel nacional.

- El Decreto 338 de 2022 de Colombia establece nuevas disposiciones para la ciberseguridad y la protección de datos personales en el país, especialmente en lo

relacionado con la gestión de incidentes de ciberseguridad y la implementación de políticas para la protección de infraestructuras críticas. Este decreto tiene como objetivo mejorar la resiliencia digital del país, fortalecer la protección de los sistemas informáticos y garantizar la seguridad en el entorno cibernético. Es un desarrollo clave.

2. Instituciones Clave

Varios organismos y entidades colombianas desempeñan un papel importante en el ámbito de la ciberseguridad:

- **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC):** Este ministerio tiene una función central en la formulación de políticas, la promoción de la ciberseguridad y la coordinación de iniciativas nacionales en la materia.

- **CERT Colombia:** El Equipo de Respuesta ante Incidentes de Ciberseguridad (CERT por sus siglas en inglés) es un organismo clave en Colombia que proporciona soporte técnico y coordina la respuesta ante incidente

3. La ciberseguridad para todos

La ciberseguridad y las crecientes dinámicas en el ciberespacio presentan cada vez más desafíos para Colombia. En ese sentido, para que la ciberseguridad esté al alcance de la población, se requieren mecanismos y buenas prácticas que sirven para la protección de IT y OT, en aras de salvaguardar la seguridad y privacidad al momento de navegar por la red.

La ciberseguridad requiere el seguimiento del modelo, el cuidado de los dispositivos, y los consejos más básicos, es relevante comprender que no se requiere grandes conocimientos técnicos, de redes o de equipos, por el contrario, la ciberseguridad es un modelo para todos.

En el presente anexo se entregan las guías básicas en ciberseguridad para poner en marcha el modelo de seguridad y privacidad de la información. Este sistema está compuesto por la identificación de activos críticos, infraestructuras críticas, la guía de gestión de incidentes y la guía de gestión de riesgos. Esta propuesta está concebida para integrar la ciberseguridad bajo un modelo que permita la gestión y anticipación de las afectaciones cibernéticas.

Lineamiento para la identificación de las infraestructuras críticas cibernéticas

Resumen ejecutivo

Las infraestructuras críticas son los sistemas físicos y virtuales esenciales que forman la espina dorsal de nuestras sociedades modernas, sirviendo de sustento para el bienestar de la sociedad en funcionamiento. Cualquier daño o interrupción de las infraestructuras críticas puede tener importantes repercusiones negativas para la seguridad de la nación. A menudo, estos sistemas se extienden más allá de las ciudades y prestan servicios a regiones enteras. En el mundo conectado de hoy, a medida que aumenta la interconexión de nuestros sistemas que son vitales para nuestra cotidianidad, también lo hacen las amenazas a las infraestructuras críticas abarcan un amplio abanico de sectores como la energía, las comunicaciones, las telecomunicaciones, el transporte, los sistemas financieros, la sanidad, el suministro de alimentos y numerosos servicios gubernamentales, estos servicios son esenciales para la vida cotidiana de los colombianos.

Dada su importancia, la protección de las infraestructuras críticas frente a posibles amenazas es una prioridad absoluta para todos los gobiernos y organizaciones del mundo. A medida que aumenta la interconexión de nuestros sistemas, también lo hacen las amenazas que son tan vitales para nuestra vida cotidiana. Estas amenazas pueden adoptar la forma de ciberataques, catástrofes naturales, sabotaje físico o muchos otros peligros. Aunque Colombia no ha dispuesto una guía oficial del “paso a paso" para la identificación de Infraestructuras Críticas, sí tenemos lecciones aprendidas de otros Estados y un trabajo de ministerio de defensa nacional que pueden ayudar mejor al establecimiento de los lineamientos para la identificación de Infraestructuras Críticas Cibernéticas.

Introducción

La norma ISO IEC 27001 hace referencia al sistema de seguridad de la información la cual incluye infraestructura crítica física, personas, información física e información digital. Así las cosas, cada uno de los elementos que conforman cada uno de estos enunciados pueden ser críticos en los casos en que se comprometa un servicio esencial para la sociedad, cuya afectación podría tener consecuencias devastadoras en la seguridad, economía, salud o bienestar de la población. Esto incluye sectores como energía, agua, transporte, salud y telecomunicaciones entre otros.

De este modo, esta guía contempla el paso a paso para la identificación critica cibernética la cual abarca los sistemas informáticos y redes que son fundamentales para el

funcionamiento de la infraestructura crítica. Esto incluye servidores, bases de datos, redes de comunicación y sistemas de control industrial. La seguridad de esta infraestructura es vital, ya que un ciberataque puede paralizar servicios esenciales y comprometer la seguridad nacional.

Englobando aquellos activos y servicios esenciales que sostienen la vida, la seguridad y el bienestar de la sociedad. Siendo la base sobre la que se construye la economía, la atención médica, la educación, la seguridad pública y muchos otros aspectos de la vida cotidiana.

En el caso de la infraestructura digital, es esencial para la seguridad nacional debido a su papel fundamental en la gestión y control de servicios críticos como el suministro de energía, el transporte y la comunicación. Sumado a la información gubernamental, financiera y personal sensible que alberga. De modo que, un ataque cibernético a la infraestructura crítica puede implicar afectaciones políticas, económicas, políticas, ambientales, entre otras, en un Estado.

Por ejemplo, un ataque cibernético puede afectar el suministro de energía eléctrica, interrumpir el transporte, causar interrupciones en las comunicaciones o afectar la prestación de servicios de atención médica. Afectando la movilidad de las fuerzas de seguridad o la capacidad del gobierno para responder a una crisis.

Por lo que la validación de los sectores y subsectores estratégicos de la infraestructura crítica es importante para la identificación y priorización de los activos y servicios críticos esenciales para el funcionamiento de la sociedad y la seguridad nacional. Lo que permite una mejor coordinación y colaboración entre las entidades públicas y privadas, así como una mayor capacidad de respuesta y resiliencia en caso de un evento disruptivo o una amenaza de seguridad.

Ambas infraestructuras requieren protección y resiliencia ante amenazas, tanto físicas como cibernéticas, y son objeto de atención por parte del gobierno y el sector privado para asegurar su funcionamiento interrumpido y su protección contra incidentes. En este contexto, este documento pretende proporcionar un marco de referencia teórico para identificar, validar y gestionar los sectores y subsectores estratégicos de la infraestructura crítica cibernética, especialmente en lo relativo a la ciberseguridad y el sector IT/OT.

En ese sentido, se toman documentos como “Cybersecurity and Infrastructure Security Agency (CISA), titulado “A Guide to Crítical Infrastructure Security and Resilience CISA 2019” de Estados Unidos.

Además, el documento incluye casos de estudio y la base teórica de metodologías internacionales que amplían la perspectiva sobre la infraestructura crítica y su importancia para la seguridad nacional. Se presentan los casos de estudio de Reino Unido, Estados Unidos, Estonia y Canadá, así como la metodología ENISA para la identificación de activos y servicios de Infraestructura de Información Crítica.

4. Normativa

En el presente estudio se han tenido como fundamento algunas normativas que establecen lineamientos generales tendientes a identificar los diferentes sectores vulnerables en las

infraestructuras críticas, tales como, el artículo 333 de la Constitución Política de Colombia[15], el cual define la empresa, como base del desarrollo económico del país, el artículo 365 de la Constitución Política de Colombia[16], que determina como finalidad social del Estado la prestación de los servicios públicos, dentro de los cuales, la Corte Constitucional en Sentencia C-691/08, ha declarado

que servicios como la banca central; el transporte; las telecomunicaciones; la explotación, refinación, transporte y distribución de petróleo y los servicios públicos domiciliarios, son materialmente servicios públicos esenciales, lo que eleva el grado de necesidad y vulnerabilidad al que pueden estar expuestos.

Por otro lado, el Consejo Nacional de Política Económica y Social, estableció mediante el Conpes 3995 de 2020, la Política Nacional de Confianza y Seguridad digital y definió como Infraestructura crítica cibernética nacional, aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.

Ahora bien, con base en lo anterior y teniendo en cuenta el principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009[17] "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las Comunicaciones - "TIC-,(...)", y debido a la imposición que tienen las entidades públicas de adoptar las medidas necesarias que les permitan garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones, el Ministerio de Tecnologías de la Información y las Comunicaciones, determinó mediante el Decreto 1078 de 2015 adicionado por Decreto 338 de 2022, la necesidad de definir la metodología para realizar el levantamiento del inventario de infraestructuras críticas cibernéticas y de servicios esenciales a cargo de las autoridades, así como, la incorporación de mejores prácticas que le sean aplicables.

5. Normativa Internacional

DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea. Establece respecto a infraestructuras con alto nivel de criticidad que:

- Las entidades incluidas en el ámbito de aplicación de la presente Directiva para gestionar riesgos de ciberseguridad deben clasificarse en dos categorías, entidades esenciales e importantes, según el grado de criticidad de sus sectores o del tipo de servicio que prestan, y de su tamaño.

- Deben considerarse debidamente las evaluaciones de riesgos sectoriales o las orientaciones de las autoridades competentes.

[15] Constitución Política de Colombia, artículo 333, (1991).
[16] Constitución Política de Colombia, artículo 365, (1991).
[17] Ley 1341 de 2009, Congreso de Colombia.

- Se han de diferenciar los regímenes de supervisión y de garantía del cumplimiento de las dos categorías de entidades para garantizar un equilibrio justo entre los requisitos y las obligaciones en función del riesgo.

- Los Estados miembros deben exigir a las entidades que presenten, al menos, la siguiente información a las autoridades competentes, a saber, el nombre, la dirección y los datos de contacto actualizados, incluidas las direcciones de correo electrónico, los rangos de IP y los números de teléfono de la entidad, y en su caso, el sector y subsector pertinente contemplados en los anexos, así como en su caso, una lista de los Estados miembros en los que prestan servicios incluidos.

- Cuando las disposiciones de un acto sectorial de la Unión exijan a las entidades esenciales o importantes que cumplan obligaciones de notificación de efecto al menos equivalente a las obligaciones de notificación establecidas en la presente Directiva, deben garantizarse la coherencia y la eficacia de la tramitación de las notificaciones de incidentes.

- Las disposiciones del acto sectorial de la Unión sobre notificación de incidentes deben proporcionar a los CSIRT, autoridades competentes o puntos de contacto únicos sobre ciberseguridad, designados con arreglo a la presente Directiva acceso inmediato a las notificaciones de incidentes presentadas de conformidad con el acto jurídico sectorial de la Unión.

- Los Estados miembros deben establecer un mecanismo de notificación automática y directa que garantice un intercambio sistemático e inmediato de información con los CSIRT, las autoridades competentes o los puntos de contacto únicos en relación con la tramitación de dichas notificaciones de incidentes sectoriales.

- Las entidades del sector de las infraestructuras digitales se basan en sistemas de redes y de información, por lo que las obligaciones impuestas a dichas entidades por esta Directiva deben abordar de manera exhaustiva la seguridad física de estos sistemas como parte de sus medidas para gestionar los riesgos de ciberseguridad y obligaciones de notificación.

- La Directiva reconoce las crecientes interdependencias son el resultado de una red cada vez más transfronteriza e interdependiente de prestación de servicios que utilizan infraestructuras clave de toda la Unión en sectores como la energía, el transporte, la infraestructura digital, el agua potable y las aguas residuales, la sanidad y determinados aspectos de la administración pública, así como el espacio en la medida en que se trate de la prestación de determinados servicios que dependen de infraestructuras terrestres.

6. Algunos sectores y subsectores con alta criticidad

Acorde al estudio preliminar se presentan algunos de los sectores y subsectores[18] con alta criticidad, estos, probablemente se actualicen con el levantamiento de la infraestructura crítica cibernética del Estado:

1. Energía

1.1 Electricidad

1.2 Sistemas Urbanos de calefacción y refrigeración

1.3 Crudo

1.4 Gas

1.5 Hidrogeno

2. Transporte

2.1. Transporte aéreo

2.2. Transporte por Ferrocarril

2.3. Transporte Marítimo
2.4. Transporte por carretera

3. Financiero

3.1 Infraestructuras de los mercados financieros

3.2 Sector sanitario

3.3 Agua potable

3.4 Aguas residuales

4. TIC

4.1 Infraestructura digital

4.2 Gestión de servicios de TIC (de empresa a empresa)

5. Estado

5.1 Entidades de la Administración pública, con exclusión del poder judicial, los parlamentos y los bancos centrales

Por consiguiente, esto es solo un ejemplo del alcance del documento, el cual tiene como objetivo exponer un análisis motivado en unos parámetros normativos que enuncian de forma general aquellas infraestructuras críticas cibernéticas y por otro lado la definición y

[18] Esto es una referencia, la criticidad de los sectores se determina con la nueva metodología. Del mismo modo, en esta se procura por la identificación de los subsectores.

el reconocimiento que se han dado de las mismas en el ámbito nacional e internacional con el fin de brindarles las herramientas precisas que conlleven asegurar la efectividad en la implementación de la metodología de las infraestructuras críticas cibernéticas y el uso de las buenas prácticas en seguridad digital.

Del mismo modo, se plantea que el levantamiento de la Infraestructura crítica Cibernética se realizará por fases:

1. **Primera fase:** Levantamiento de Infraestructura Crítica Cibernética y clasificación de la criticidad en los sectores. (Se identifican los subsectores a nivel general)

2. **Segunda fase:** Levantamiento de la Infraestructura Crítica Cibernética en los Subsectores e identificación de los operadores.

3. **Tercera Fase:** Levantamiento de la Infraestructura Crítica Cibernética de los operadores.

La propuesta se actualizará cada 02 años, y se procura por partir de lo general a lo particular, estableciendo los principales riesgos y amenazas sobre la Infraestructura Crítica Cibernética.

7. Antecedentes de las Infraestructuras Críticas y su metodología en Colombia

Algunos países han adoptado una estructura similar de sectores críticos, como la utilizada por los Estados Unidos, hay diferencias en la forma en que se agrupan los subsectores y la forma en que se gestionan los riesgos y amenazas específicas de cada sector. En Colombia, esta información se empieza a desarrollar con la primera versión del Catálogo Nacional de Infraestructuras Críticas Cibernéticas V1.0 [1].

Esta nace con el propósito de definir los sectores estratégicos de Colombia, para realizar la identificación de la infraestructura crítica cibernética del país, en el marco del manejo de riesgo operacional nacional, la ciberseguridad y la ciberdefensa y en su momento estas actividades lideradas por el comando conjunto cibernético coordinación con el equipo de respuesta a emergencias cibernéticas de Colombia quien hacia parte del ministerio de defensa nacional.

En ese sentido, se procedió a la construcción de un documento que serviría como referencia a todas las entidades publico privadas o de economía mixta que cuente con infraestructura de tecnologías de información de comunicaciones o tecnologías de operación.

El 31 de octubre de 2012 se activa con el primer congreso de ciberseguridad llevado a cabo en las instalaciones del hotel capital en Bogotá y con la creación del Comando Conjunto Cibernético de las Fuerzas Militares, y cumpliendo con lo dispuesto en el documento CONPES 3701 de 2011 en donde se debía realizar con el COLCERT la identificación y taxonomía de las infraestructuras críticas cibernéticas en Colombia.

Con la autorización del ministerio de defensa en donde se encontraba la dirección del COLCERT, se procedió a realizar la primera fase para que el Comando Conjunto Cibernético de las Fuerzas Militares realice la convocatoria de los responsables y dueños de las infraestructuras críticas cibernéticas para iniciar con las reuniones pertinentes. Así pues, se realizó una lista de contactos y un inventario de estas y fijar

unos criterios de periodicidad de las reuniones hasta culminar el proceso de realizar la identificación y elaborar una cartilla de los sectores de infraestructura crítica cibernética que existen en Colombia.

Así mismo se realizó el cronograma de reuniones una por mes y se definió en el cronograma anual el cual era aprobado por los mismos participantes en las reuniones de infraestructuras críticas cibernéticas.

Teniendo en cuenta los puntos anteriores de organización se desarrollaron las mesas de infraestructura críticas cibernéticas, en ellas se empezó a trabajar en la metodología. Es importante resaltar que inicialmente asistieron gran número de sectores entre otros COLCERT, Isagen, Bancolombia, Universidad de los Andes, Empresas Públicas de Medellín, Instituto Tecnológico De Medellín, Asobancaria, Banco Bilbao Vizcaya Argentaria, Ministerio De Comunicaciones, Ministerio De Justicia, Diferentes Empresas Del Sector De La Tecnología, Isa, Registro Único de Tránsito, Acueducto Bogotá, Departamento Nacional de Planeación, Pacific Rubiales, Davivienda, Banco De La República, Presidencia De La Republica CSIRT-Gobierno, Ecopetrol, Aeronáutica Civil, XM, entre otros.

La taxonomía en Colombia, para este estudio se realizó tomando como referencia la metodología aplicada por la Unión europea para la identificación de la taxonomía en el país estableciendo los niveles y subniveles de categorización de la infraestructura colombiana de forma jerárquica basado en sectores y subsectores.

Los 13 sectores elegidos se basan en la propuesta del Catálogo Nacional de Infraestructura Crítica Cibernética (CNICC), el cual fue un estudio realizado en 2015 a una muestra de más de 90 empresas e instituciones del sector público, privado y mixto, con el fin de determinar el listado priorizado de instituciones, entidades y empresas que ostentan la responsabilidad de garantizar el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos y la defensa nacional.

Dicho catálogo en su primera versión fue el resultado de treinta y siete (37) meses de trabajo continuo del Ministerio de Defensa Nacional en coordinación con otros ministerios, y con la participación de varias empresas e instituciones representativas de los sectores público, privado, la academia y la sociedad civil a fin de garantizar, se contara una visión y un análisis holístico y complementario para estudiar los sectores estratégicos del país que cuentan con oportunidades de desarrollo, consolidación y brindan un aprovechamiento a través de plataformas tecnológicas de información o de operación y mantienen potencialidades de crecimiento sustentable en el largo plazo y la posterior identificación de Infraestructura Crítica Cibernética (ICC).

Estos sectores seleccionados se basan en el estudio ya realizado de “los sectores Estratégicos de la República de Colombia desde la óptica Cibernética”: el cual en 2015 estableció los trece sectores de estudio en los cuáles se aplicará la actualización metodológica de la ICC del país y el impacto que tiene el componente cibernético y el ciberespacio en la prestación de los servicios esenciales a la población en cada uno de los

sectores. En este sentido, los 13 sectores nacen del trabajo ya realizado, y son los que serán adoptados por la propuesta de metodología que se actualiza para 2024.

1. Alimentación Y Agricultura

2. Agua

3. Comercio, Industria, Turismo

4. Defensa

5. Educación

6. Electricidad

7. Financiero

8. Gobierno/Estado

9. Recursos Naturales-Medio Ambiente

10. Recursos Minero-Energéticos

11. Salud Y Protección Social

12. Tecnologías De La Información Y Comunicaciones

13. Transporte

Durante el desarrollo de las mesas de trabajo se realizó una clasificación por sectores, la cual dio la elaboración del borrador de la guía para la definición de infraestructuras críticas digitales en Colombia, entre los años 2013, 2014, 2015 y finalizando el 2016 se cumplió con la elaboración de la cartilla en donde se definieron los 13 sectores de infraestructura crítica para Colombia**.**

Es importante anotar que, en el trabajo realizado, las mesas identificaron, priorizaron y catalogaron las infraestructuras críticas digitales y así mismo se determinó que las IC eran interdependientes, complementarias y heterogéneas entre las mismas, conceptos que se llevaron a cabo gracias a la metodología empleada.

En conclusión, el trabajo del primer catálogo fue el desarrollo del trabajo de Infraestructuras críticas cibernéticas que se realizó desde 2016 y es la base de la actualización metodológica que aborda el presente documento.

8. Roles y responsabilidades con la Ciberseguridad y Ciberdefensa de la infraestructura crítica cibernética:

Los roles y responsabilidades en cuanto a la seguridad digital (ciberseguridad) y ciberdefensa de la infraestructura crítica cibernética pueden variar entre países, y esto depende del

contexto y la estructura de gobernanza de cada país. En algunos países, la responsabilidad de la protección de la infraestructura crítica puede estar centralizada en una entidad específica, como un departamento de seguridad nacional o un organismo regulador. En otros, las responsabilidades pueden ser compartidas entre varias entidades, incluidos los sectores público y privado.

En el caso de Colombia, se reconoce que, aunque la Ciberseguridad y Ciberdefensa son responsabilidad de todos, cada uno de los trece sectores debe contar con un delegado visible, en ese sentido se plantea que el líder de cada sector sea el oficial de seguridad o el jefe de la oficina de TI quienes son los encargados de supervisar, coordinar y garantizar la seguridad, continuidad y eficiencia de un conjunto de servicios o sistemas esenciales para el funcionamiento del sector, asegurando su

información; así pues, esto se alinea a los mismos representantes del Comité Nacional de Seguridad Digital.

Igualmente, se requiere que cada sector cree un buzón de correo con la siguiente estructura seguridad.ciber@entidad.gov.co ejemplo: (seguridad.ciber@mintic.gov.co), esto para mantener una comunicación fluida y generar mayor sinergia:

Sector	Representante del Sector	Usuario/Contacto
1) Alimentación Y Agricultura	Ministerio de Agricultura	
2) Agua	Ministerio de Ambiente	
3) Comercio, Industria y Turismo	Ministerio de Comercio, Industria y Turismo	
4) Defensa	Ministerio de Defensa	
5) Educación	Ministerio de Educación	
6) Electricidad	Ministerio de Minas y Energías	
7) Financiero	Ministerio de Hacienda	
8) Gobierno/Estado	Presidencia de la República/Función Pública	
9) Recursos Naturales-Medio Ambiente	Ministerio de Ambiente	
10) Recursos Minero-Energéticos	Ministerio de Minas y Energía	
11) Salud Y Protección Social	Ministerio de Salud y Protección Social	
12) Tecnologías De La Información Y Comunicaciones	Ministerio TIC	
13) Transporte	Ministerio de Transporte	

Tabla 21 Sectores y sus responsables

Fuente. Construcción Propia

La entidad líder encargada de la gestión de la Infraestructura Crítica Cibernética (ICC) es clave para coordinar y supervisar las acciones relacionadas con la protección de las infraestructuras críticas del sector. A continuación, se detallan las características, roles y funciones de dicha entidad líder:

Características de la Entidad Líder de ICC del sector.

- La entidad debe tener un mandato legal claro y la autoridad necesaria para establecer y hacer cumplir políticas y regulaciones de ciberseguridad.
- Debe contar con los recursos técnicos y humanos necesarios para desarrollar e implementar estrategias de ciberseguridad a nivel de las entidades del sector.
- Capacidad para coordinar y colaborar eficazmente con otras entidades gubernamentales, el sector privado y organizaciones internacionales.
- Compromiso con la transparencia en sus operaciones y la responsabilidad en la gestión de la seguridad cibernética.

Roles de la Entidad Líder de ICC del sector.

- Actuar como la entidad reguladora que establece normas y supervisa su cumplimiento en materia de seguridad cibernética.
- Funcionar como el centro de coordinación para la respuesta a incidentes cibernéticos a nivel de las entidades del sector.
- Promover la colaboración y el intercambio de información entre diferentes sectores y actores relevantes.
- Proporcionar recursos, apoyo técnico y capacitación a las entidades del sector para mejorar sus capacidades de ciberseguridad.
- Realizar evaluaciones periódicas de los riesgos cibernéticos a nivel de las entidades del sector y proporciona directrices para la mitigación de estos riesgos.

Funciones de la Entidad Líder de ICC del sector

- Desarrollar y actualizar políticas, normas y guías de ciberseguridad para la protección de infraestructuras críticas, asegurando que estas políticas sean adoptadas por las entidades del sector.
- Establecer criterios y participar en la creación o adaptación de metodologías para la identificación y clasificación de infraestructuras críticas cibernéticas, manteniendo un registro actualizado de las infraestructuras críticas a de las entidades del sector.
- Realizar evaluaciones de riesgo a nivel de las entidades del sector para identificar amenazas y vulnerabilidades que puedan afectar a las infraestructuras críticas, desarrollando estrategias y planes de mitigación de riesgos.
- Establecer un monitoreo de ciberseguridad para detectar y responder a incidentes cibernéticos, coordinando la respuesta a incidentes a nivel de las entidades del sector, incluyendo la comunicación y colaboración con entidades afectadas y otros actores relevantes.

- Desarrollar programas de capacitación en ciberseguridad para las entidades del sector, mediante campañas de concientización sobre la importancia de la seguridad cibernética y las mejores prácticas.

- Facilitar la colaboración y el intercambio de información entre entidades gubernamentales, el sector privado y organizaciones internacionales, facilitando la realización de foros y grupos de trabajo de ciberseguridad a nivel sectorial e internacional.

- Proporcionar retroalimentación y apoyo para mejorar las prácticas de ciberseguridad en las entidades del sector.

- Propender por la inversión en el desarrollo y mantenimiento de infraestructuras tecnológicas avanzadas para la protección de infraestructuras críticas en las entidades del sector.

- Fomentar la investigación y desarrollo en ciberseguridad para estar a la vanguardia de las tecnologías y amenazas emergentes en las entidades del sector.

Es importante indicar que la entidad líder de ICC del sector juega un papel fundamental en la protección de la infraestructura crítica cibernética del sector,

asegurando que las entidades del sector cuenten con el apoyo, la orientación y los recursos necesarios para enfrentar las amenazas cibernéticas de manera eficaz.

Del mismo modo, es preciso establecer algunos roles y responsabilidades específicas que permitan armonizar los planes y estrategias previstas para tal fin [2]:

a. Gobierno: Ser referente y modelo a seguir en el buen uso del ciberespacio y en la aplicación de las buenas prácticas en Ciberseguridad y Ciberdefensa.

- El Equipo de Respuesta a Emergencias Cibernéticas COLCERT, responsable de la coordinación nacional en materia de gestión de incidentes y seguridad digital.

b. Sector Público: Liderar política pública y establecer el MSPI así como alinear un modelo para protección y defensa para las Infraestructuras Críticas Cibernéticas; bajo altos esquemas de Ciberseguridad y Ciberdefensa para las infraestructuras críticas y la sociedad en general.

c. Empresas Privadas y Mixtas: Adoptar y tomar medidas de operadores alineados una conciencia y cultura de Ciberseguridad, así como adoptar el MSPI y las políticas y guías para dar respuesta ante afectaciones a la seguridad digital. Este actor es fundamental, ya que no solo debe cumplir el MSPI, sino debe articularse con el sector público.

d. Propietarios y/o Operadores de Infraestructura Crítica Cibernética: Trabajar de la mano con las autoridades de Ciberseguridad y Ciberdefensa, así como desarrollar y aplicar planes de protección y defensa.

e. Sector Defensa:

- **El Comando Conjunto Cibernético (CCOCI):** Será responsable de la Ciberdefensa Nacional.

- **El Centro Cibernético Policial de la Ciberseguridad Ciudadana:** Quienes trabajarán de manera coordinada a fin de focalizar esfuerzos y minimizar los riesgos cibernéticos que puedan afectar la Seguridad y Defensa Nacional.

f. Agencias de Inteligencia: Fortalecer las capacidades de inteligencia y contrainteligencia en el ciberespacio para proteger los derechos y libertades de los ciudadanos y de las personas residentes en Colombia, así como identificar oportunidades y riesgos, al igual que identificar, conocer y contrarrestar amenazas internas o externas contra el bienestar de los colombianos, la vigencia del régimen democrático, el orden constitucional y legal, la seguridad y la defensa nacional.

g. Academia y Centros de Investigación: Fortalecer la capacitación en Ciberseguridad y Ciberdefensa a todo nivel.

h. Agremiaciones: Gestionar con sus asociados la aplicación de buenas prácticas y medidas de Ciberseguridad y Ciberdefensa.

9. Sectores Críticos Nacionales 2024

1. **Sector:** Alimentación y agricultura

En Colombia, hoy, esto se refiere a todas las actividades agropecuarias como alimentos, piensos, ganado y técnicas para la cría. Colombia es uno de los principales productores de café, aceite de palma y caña de azúcar del mundo. Se espera que el mercado agrícola colombiano crezca un 7% para 2028, totalizando alrededor de 14 mil millones de dólares.

2. **Sector:** Agua

a. Colombia posee actualmente algunos de los mayores depósitos de recursos de agua dulce del mundo. La capacidad de suministrar agua potable limpia y segura es una estructura crítica para una sociedad sana y productiva.

3. Sector: Comercio, Industria y Turismo

a. Colombia sigue fomentando ser un destino líder para los viajes internacionales y un socio cada vez más vital para la inversión del sector privado. El crecimiento económico del comercio ha visto un aumento en varios sectores en Colombia, permitiéndole ser un exportador e importador de varios productos a través del mundo.

4. Sector: Defensa

a. La industria de Defensa se compone de varios sectores interconectados, como el tecnológico, el financiero y el comercial. Este sector ayuda a posibilitar actividades de investigación y desarrollo en varios sectores. El Ministerio de Defensa es el principal organismo gubernamental de este sector y está compuesto por el Ejército Nacional, la Armada, la Fuerza Aéreo Espacial colombiana y la Policía Nacional.

5. **Sector:** Educación

a. El Sector Educativo es la base para proporcionar habilidades relevantes, así como un camino hacia futuras oportunidades para los ciudadanos de toda Colombia. La capital cuenta con más de 30 universidades que reciben candidatos de todo el mundo. El Ministerio de Educación esbozó áreas clave para que Colombia sea "El país con más educación de América Latina en 2025".

6. **Sector:** Electricidad

a. La gran mayoría del sector eléctrico en Colombia se genera a través de energía hidroeléctrica y térmica. Este sector depende en gran medida de los socios del sector privado para trabajar con los organismos gubernamentales en el suministro de energía fiable a la red crítica nacional. La mayor parte de esta energía se utiliza para el consumo residencial e industrial.

7. **Sector:** Financiero

a. El sector financiero es una parte clave del buen funcionamiento de la sociedad. Los ataques o compromisos al sector financiero pueden debilitar las funciones críticas nacionales de Colombia.

8. **Sector:** Gobierno/Estado

a. El sector público ayuda a las distintas partes interesadas a comprender mejor los riesgos de sus carteras específicas. El sector gubernamental incluye entidades del sector público y entidades descentralizadas a nivel departamental, municipal y verdal que se apoyan en una fuerte asociación para asegurar mejor sus sistemas.
b. En este sector se encuentran los organismos de control, la rama legislativa, judicial, los concejos distritales y municipales y organismos de control como Procuradurías, veedurías, personerías, contralorías, etc.

9. **Sector:** Recursos Naturales-Medio Ambiente

a. El sector de Medio Ambiente y de manejo de recursos naturales resulta extremadamente importante para las Funciones Críticas Nacionales. Siendo Colombia uno de los países con mayor biodiversidad del mundo, este sector proporciona una gran riqueza de recursos al desarrollo estatal.

10. **Sector:** Recursos Minero-Energéticos

a. **El sector minero-energético** se compone de diversas industrias productoras de energía como el sector minero y de extracción de metales, y la industria de petróleo y gas. Este sector actúa como multiplicador de la Economía nacional, ya que en el país para el 2021 se tuvieron exportaciones de petróleo crudo de 26%, de carbón de 12% y de oro de 6.14%.

11. **Sector:** Salud y Protección Social

a. Los sectores de Salud y Protección Social prestan un servicio crítico para proteger el bienestar y la salud de todos los sectores de la economía. Están preparados para apoyar cualquier amenaza natural, humana o terrorista contra la población de Colombia.
b. La pandemia de COVID-19 ilustró cómo la salud y la seguridad de la población de un país son fundamentales para su funcionamiento cotidiano. El sector sanitario depende en gran medida de las relaciones intersectoriales para asegurar mejor sus infraestructuras críticas.

12. **Sector:** Tecnologías de la información y comunicaciones
a. Cada vez son más los países que digitalizan sus numerosos sectores, por lo que nunca ha sido tan importante proteger estas infraestructuras críticas de los malos agentes y las amenazas.
b. La dependencia de las tecnologías de la información es cada vez mayor a medida que nos interconectamos. Las interdependencias inherentes al sector de las tecnologías de la información han creado retos únicos en materia de protección, pero también nuevas oportunidades de colaboración.

13. **Sector:** Transporte
a. El sector del transporte asiste a millones de colombianos que viajan por el país cada día, y a bienes y servicios económicos, como petróleo, productos agrícolas, café y madera.
b. El sector del transporte es una función crítica nacional que, si se interrumpe, tendrá amplias repercusiones en otros sectores interconectados como la salud y la seguridad, el comercio, la tecnología y la defensa.

Ahora bien, de acuerdo con el decreto 338 de 2022, el Ministerio de Tecnologías de la Información y las Comunicaciones convoca a cada uno de los sectores catalogados como titulares de infraestructura crítica cibernética o de servicios esenciales dentro del presente documento, para que designen un representante, quien será presentado como tal, mediante escrito dirigido al Ministerio de tecnologías de la información y las comunicaciones y el Comité Nacional de Seguridad Digital antes del 30 de agosto de 2024, para luego ser convocado en las mesas sectoriales de Infraestructuras Críticas Cibernéticas - ICC que se realizaran con ocasión a la verificación y seguimiento del levantamiento de las ICC.

10. Amenazas y Riesgos a la infraestructura crítica digital

La Cuarta Revolución Industrial, caracterizada por la convergencia de tecnologías digitales, físicas y biológicas, ha traído consigo avances sin precedentes. Sin embargo, esta transformación digital también ha introducido amenazas y riesgos nuevos y complejos que requieren seria atención.

Entre las amenazas y riesgos específicos figuran los relacionados con la Inteligencia Artificial, las comunicaciones 5G, la analítica de datos y el Big Data, y otras tecnologías emergentes. Los sesgos algorítmicos en los sistemas de IA pueden perpetuar y amplificar los sesgos existentes, dando lugar a decisiones injustas y discriminatorias. El desarrollo de sistemas de armas autónomas también plantea graves problemas éticos y de seguridad.

Además, la automatización que permite la IA puede desplazar a un número significativo de trabajadores, alimentando el desempleo y la desigualdad (The Fourth Industrial Revolution, 2017). El auge de los «deepfakes» -contenidos falsos de gran realismo- puede manipular la opinión pública y socavar la confianza en las instituciones (Konina, 2021)(Velarde, 2020)(Agbaji et al., 2023).

El aumento de la conectividad y la dependencia de las redes 5G las hacen más vulnerables a los ciberataques, lo que plantea riesgos para la privacidad y puede interferir con sistemas críticos (Thomaz et al., 2021)(Velarde, 2020)(La Cuarta Revolución Industrial, 2017). La recopilación y el análisis masivos de datos personales a través de Big Data también plantean problemas de privacidad, y la manipulación de los datos puede utilizarse para influir en la opinión pública y en los procesos electorales.

La proliferación de dispositivos del Internet de las Cosas aumenta la superficie de ataque y la probabilidad de ciberataques, mientras que la tecnología blockchain, aunque ofrece ventajas de seguridad y transparencia, también puede ser explotada. Estos son algunas de las amenazas y riesgos que se tratan dentro del MSPI, el cual es la base de este documento.

a. Riesgos a la infraestructura crítica cibernética

La definición de los riesgos a la infraestructura crítica cibernética se da con base en el Modelo de Seguridad y Privacidad de la Información (MSPI) el cual fue actualizado y toma en cuenta los modelos europeos. En ese sentido se plantean los principales riesgos.

b. Amenazas a la infraestructura crítica cibernética

La infraestructura crítica ha estado sujeta durante mucho tiempo a **amenazas físicas y desastres naturales**, y ahora también está cada vez más expuesta a **riesgos cibernéticos**. Estos riesgos se derivan de una creciente integración de las tecnologías de la información y las comunicaciones con la infraestructura crítica y los adversarios centrados en explotar las posibles vulnerabilidades cibernéticas. A medida que la infraestructura física se vuelve más dependiente de sistemas cibernéticos complejos para las operaciones, la infraestructura crítica puede volverse más vulnerable a ciertas amenazas cibernéticas, incluidas las **amenazas transnacionales**.

Las amenazas y los peligros pueden ser específicos de regiones geográficas o de todo un país, e incluso pueden tener ramificaciones globales como:

- **Eventos Climatológicos:** temperaturas extremas, sequía e incendios forestales.
- Eventos Hidrológicos: inundaciones
- **Eventos Meteorológicos**: ciclones tropicales, severas, invierno severo etc.
- **Eventos Geofísicos:** terremotos, tsunamis y erupciones volcánicas
- **Pandemias:** brotes de enfermedades globales.
- **Accidentes Tecnológicos e Industriales:** fallas estructurales, incendios industriales, riesgos emisiones de sustancias y derrames químicos.

- **Interrupciones no programadas**: infraestructura obsoleta, mal funcionamiento del equipo y fallas a gran escala.

- **Incidentes Criminales y Ataques Terroristas:** vandalismo, robo, daños a la propiedad, incidentes de disparos y ataques cinéticos.

- **Incidentes cibernéticos**: ataques de denegación de servicio, malware, phishing, entre otros.

- **Ataques a la cadena de suministro**: explotación de vulnerabilidades para causar fallas en el sistema o la red.

- **Operaciones de influencia extranjera:** para difundir información errónea o socavar procesos

- Inversión no confiable: para dar potencialmente a las potencias extranjeras una influencia indebida sobre la infraestructura critica del país

11. Derechos comprometidos por las ICC.

La seguridad nacional requiere la protección de una serie de infraestructuras que resultan fundamentales para el mantenimiento de servicios esenciales de la comunidad, cuya interrupción tendría graves consecuencias para territorios concretos o para el país en general lo que coyunturalmente generaría una afectación a los derechos de los ciudadanos, entre los cuales prima el Derecho a la vida y sus derechos conexos como el Derecho a la salud, al agua y saneamiento, alimentación, Derecho a la libertad seguridad e integridad personal, Derecho al trabajo, Derecho a los servicios públicos domiciliarios, Derecho a la prestación del servicio público de transporte, entre otros.

De este modo, la implementación de la metodología de identificación de las ICC en conjunto con las guías de activos, gestión de riesgos y gestión de incidentes, facilitan el éxito del levantamiento de las ICC y la generación oportuna de acciones y operaciones según la dinámica de los riesgos que permitan establecer lineamientos en donde prime la seguridad de las ICC y los servicios esenciales para que sean aprovechados activa y correctamente en beneficio de los derechos de los ciudadanos.

Este enfoque basado en la prevención desde la identificación busca fomentar la confianza en el entorno digital, el fortalecimiento en el sector económico y social, lo que permitirá asegurar la prestación de los servicios esenciales, la innovación, productividad, competitividad, empleo y sobre todo una vida digna en un entorno seguro en el cual se evite la materialización de infracciones a los derechos de los ciudadanos.

Las infraestructuras críticas cibernéticas protegen varios derechos humanos fundamentales, entre ellos:

1. Derecho a la vida y la seguridad: La identificación y protección de sistemas que pueden afectar la prestación esencial de servicios como la energía, el agua y la salud entre otros, asegura que las personas puedan acceder a servicios vitales, previniendo riesgos asociados a la vida e integridad de las personas.

2. Derecho a la privacidad: La identificación de las infraestructuras criticas cibernéticas permite la implementación de controles oportunos para la protección de los datos personales y datos sensibles de los individuos frente accesos no autorizados.

3. Derecho a la libertad de expresión: La protección de las infraestructuras cibernéticas también asegura que las plataformas de comunicación y expresión no sean censuradas o manipuladas, permitiendo el libre flujo de información.

4. Derecho a la información: Mantener la seguridad de las infraestructuras críticas cibernéticas asegura que la información sobre servicios públicos y emergencias esté disponible y sea accesible, a su vez proporciona que las personas puedan recibir la información clara, oportuna y veraz.

5. Derecho a la seguridad: La ciberseguridad protege a las personas y sociedades de amenazas cibernéticas que pueden causar daños físicos o emocionales. La seguridad en el ciberespacio es una extensión del derecho a vivir en un entorno seguro.

6. Igualdad y no discriminación: La identificación de las ICC permiten tomar acciones dentro del estado de manera que no discriminen a ningún grupo, garantizando que todos tengan acceso igualitario a la tecnología, a la información, a la educación digital y a la protección contra ciberamenazas, entre otras situaciones de desarrollo que se generaron dentro de los ecosistemas digitales.

El equilibrio entre la ciberseguridad y la protección de los derechos fundamentales es crucial para garantizar que las medidas de seguridad no se conviertan en herramientas de control o represión; En este sentido, es fundamental la identificación de las ICC y la implementación de los controles para generar medidas proactivas por parte de los administradores y el gobierno.

12. Casos comparados: Metodología Infraestructura Crítica Cibernética

El estudio de casos comparado de metodologías de infraestructura crítica cibernética revela los diversos enfoques para identificar, evaluar y mitigar amenazas y riesgos en los activos críticos. Si bien comparten variables comunes, se debe garantizar la resiliencia y continuidad operativa, cada metodología difieren en su alcance, profundidad y énfasis en aspectos como la evaluación de riesgos, la gestión de incidentes y la gobernanza. El presente análisis y el anexo 3 identifican os enfoques, las variables y los sectores principales en cada Estado, esto vario acorde a cada realidad o entidad.

Actor	Documento	Metodología	Variables	Sectores
ENISA	Methodologies for the identification of Critical Information Infrastructure assets and services	**1. Enfoque no dependiente del servicio crítico:** No implica un análisis de los servicios críticos soportados; en su lugar, solo analiza la infraestructura de la red. **2. Enfoque dependiente de los servicios críticos (CS):** Comienzan con la identificación de los servicios críticos y los servicios que pertecen a estos. Se basa en el impacto que la interrupción de un servicio puede tener en las funciones vitales de la sociedad	**1.** Tamaño de la población afectada **2.** La dependencia intersectorial **3.** El impacto geográfico **4.** La seguridad personal y el impacto en la privacidad	
Laboratorio Nacional de Argonne de los Estados Unidos	Metodología para evaluar las interdependencias y dependencias de la infraestructura critica	**1. Estimación Inicial:** Recopilación de información general de los activos de infraestructura crítica utilizando fuentes abiertas. **2. Actual:** Recopilación y análisis de datos de las dependencias físicas, cibernéticas y geográficas, utilizando herramientas de anticipación y visualización. **3. Avanzada:** Estudio de sistemas de infraestructuras críticas, con nuevos mecanismos de recopilación de datos e integración de herramientas **4. Objetivo Final:** Comprensión integral de todas las dimensiones de dependencia e interdependencia,		

OCDE	Metodología de la OCDE para la identificación de infraestructuras criticas	**1.** Identificar activos y redes críticas con evaluación de criticidad. **2.** Análisis de interdependencias **3.** Realización de análisis de vulnerabilidad para identificar puntos débiles (Uso de metodología CRISRRAM, RAMCAP Plus)		
Canadá	National Estrategy for Critical Infraestructure		Procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para: 1.La Salud 2. Bienestar economico 3. Seguridad 4. Efectividad en el funcionamiento del gobierno	Energía y servicios Públicos Finanzas Alimento Transporte Gobierno Tecnología de la información y la comunicación Salud Agua Seguridad Fabricación
Australia	Critical Infraestructure resilence strategy		Impacto en: - El bienestar social - El bienestar económico - La seguridad y defensa nacional	Energía Agua Transporte Comunicaciones Bancos y finanzas Salud Alimento Educación superior e investigación Servicios de emergencia Defensa Espacio
Estados Unidos	Framework for Improving Critical Infrastructure Cybersecurity (NIST)	**1. Gestión de activos:** se identifican los dispositivos, sistemas físicos, datos, software, aplicaciones y sistemas de comunicación dentro del sector. **2. Definición de operadores y proveedores:** se definen los operadores y proveedores del sector y se identifica un socio externo del que depende esa infraestructura. **3. Evaluación de riesgos:** se identifican y documentan las vulnerabilidades de los activos críticos cibernéticos, se identifican y	Impacto en: 1. La seguridad de la nación 2. La Seguridad Económica Nacional 3. La Salud 4. La Seguridad Publica 5. La Seguridad Cibernética y Privacidad 6. La Gobernanza en Ciberseguridad	Tecnología de información TI Sistemas de Control Industrial Sistemas ciberfisicos Internet de las Cosas IoT
Suiza	The Swiss National Strategy for the Protection of Critical Infrastructure	**1.** Realización de una evaluación de riesgos **2.** Análisis de la importancia de cada infraestructura crítica **3.** Evaluación de la vulnerabilidad de cada infraestructura crítica **4.** Elaboración de una lista de infraestructuras críticas prioritarias	Impacto en: 1. El bienestar social 2. La economía 3. La seguridad nacional	Energía Transporte Tecnologías de la información y la comunicación (TIC) Servicios financieros Administración pública Salud pública Seguridad pública Agua Alimentación

Reino Unido	Critical National Infrastructure	1. Mapear funciones esenciales con base a las variables establecidas 2. Determinar los sistemas: Mapear los sistemas que proporcionan la función 3.Evaluar los impactos del sector en el sistema de infraestructurasx 4. Identificar los sistemas, las organizaciones y las relaciones de apoyo 5. Evaluar los impactos intersectoriales	Impacto en: 1. La sociedad 2. Económia 3. Defensa y seguridad nacional 4. Indice demografico	Quimicos Nuclear civil Comunicaciones Defensa Servicios de emergencia Energía Finanzas Alimento Gobierno Salud Espacio Transporte Agua
Portugal	Ranking Critical Infrastructures – The Portuguese Methodology	1. Se identifican las infraestructuras críticas y se clasifican según su sector. 2. Análisis de Interdependencia y efecto cascada por medio del algoritmo ADPA y las construcción de una matriz de dependencias 2. Se evalúa la criticidad de cada infraestructura crítica mediante la identificación y análisis de los impactos potenciales de un evento adverso en la sociedad y la economía. 4. Se priorizan las infraestructuras críticas en función de su importancia relativa	Impacto en: 1. La seguridad pública 2. La economía 3. El medio ambiente 4. La sociedad	Energía Transporte Abastecimiento de agua Salud Comunicaciones Banca y finanzas Administración pública Industria química Industria nuclear Defensa Alimentación

Ilustración 1 Comparativo de metodología de ICC internacional

Fuente: Construcción Propia

13. Metodología para identificación de ICC en Colombia

Según la línea expuesta el presente documento plantea una actualización de la metodología, la cual requiere identificar las infraestructuras críticas cibernéticas a través del paso a paso expuesto a continuación, para así, lograr el levantamiento del inventario de ICC y de servicios esenciales en el ciberespacio. En esta parte se explica cómo se llega a la identificación de las variables y en el capítulo posterior, se explica el paso a paso y los productos a lograr mediante el levantamiento de ICC.

Paso 1. Identificar el problema: identificación del problema donde sectores deben abordar y desarrollar un concepto que puedan ejecutar juntos. Para ello se debe:

1.1. Identificación de la agencia líder: Necesidad de definir qué agencia o departamento gubernamental liderará este esfuerzo. Durante este proceso, debe haber una comprensión de la cantidad de recursos y tiempo necesarios para completar esta tarea. La Agencia/Departamento coordinador también deberá elegir un "Líder del Equipo de Planificación". Una vez hecho esto, deberán revisar cualquier documentación o gobernanza actual existente.

a. Definir los apoyos: Para la identificación de apoyos se debe identificar la dependencia e interdependencia entre los sectores. Como existe un alto nivel de las relaciones físicas

comunes entre los sistemas de infraestructura crítica, se hace necesario definir las dependencias de alto nivel para definir los sectores de interés.

En la siguiente ilustración se relacionan las dependencias en un alto nivel, los puntos rojos indican que el sector de apoyo identificado en la parte superior de la columna proporciona bienes o servicios al sector de interés a lo largo del lado izquierdo de la matriz.

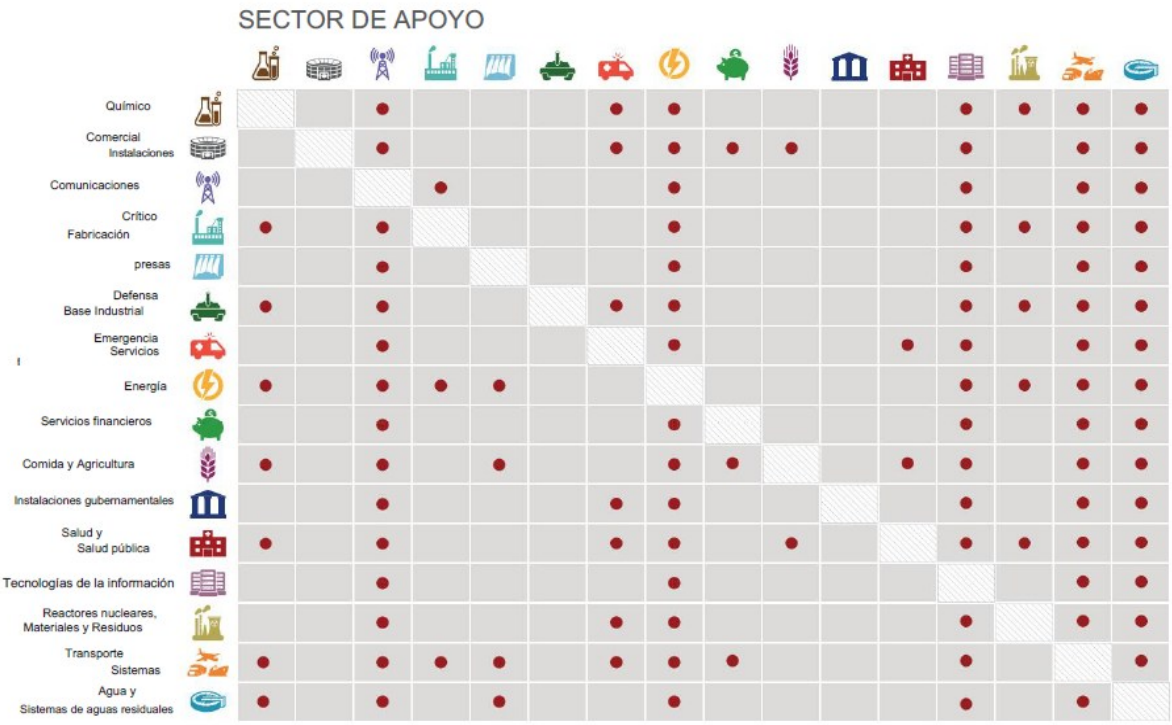


Ilustración 2 Interdependencia de Infraestructura Crítica Cibernética de Estados Unidos

Fuente. CISA.

En el caso de Colombia se propone esta interrelación la cual vario acorde al levantamiento y actualización en el levantamiento de la Infraestructura Crítica cibernética. Este paso se identifican los 13 sectores y acorde al tercer paso del Excel, se explica la interrelación que se pretende lograr a partir del levantamiento de la ICC.

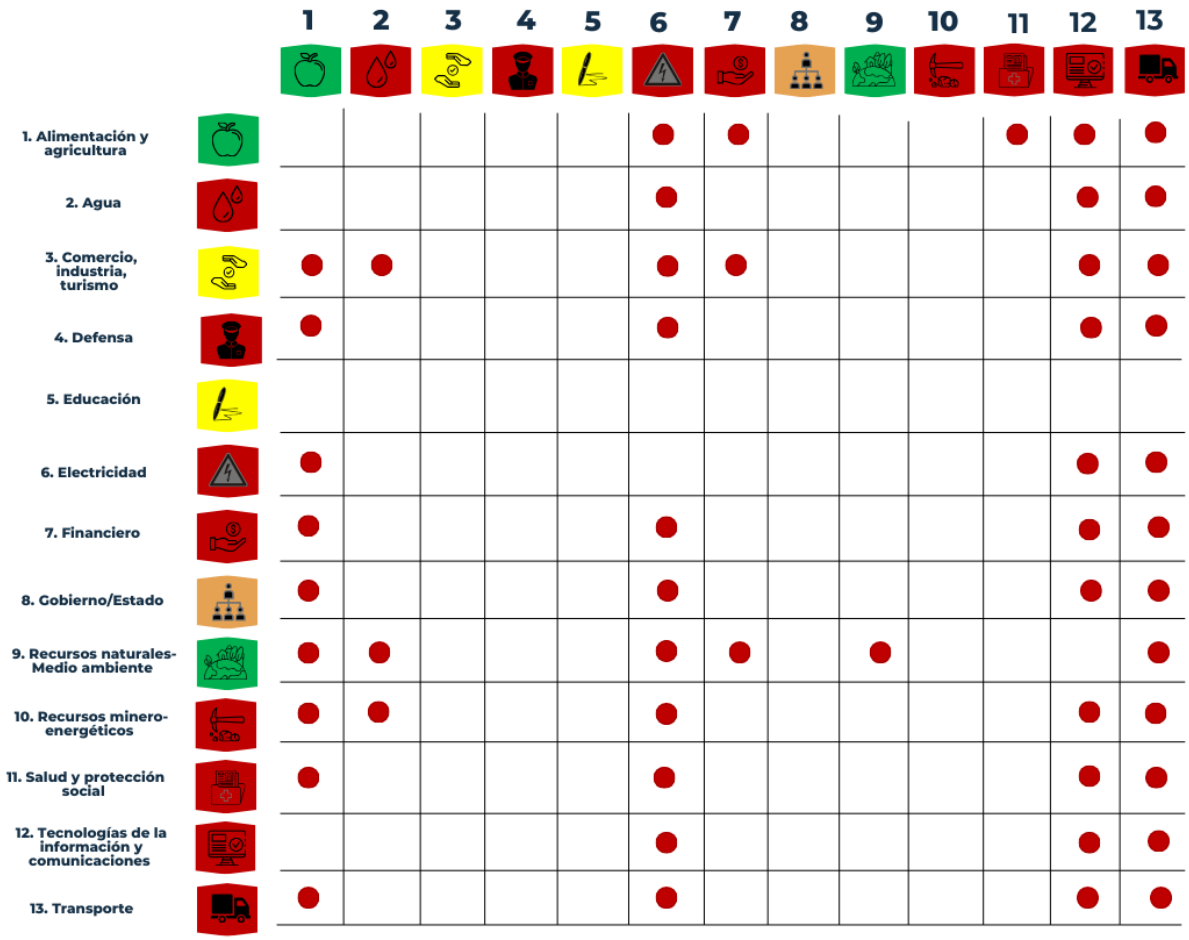


Ilustración 3 Interdependencia de infraestructura Crítica Cibernética de Colombia

Fuente. Construcción propia

b. **Identificar conceptos:** Se deben reflejar un cierto grado de investigación fundamental realizada por las principales partes interesadas para confirmar la necesidad de una evaluación y la viabilidad de los primeros conceptos propuestos.

c. **Experiencia pasada con incidentes del mundo real:** se deben analizar los huracanes, incendios forestales, ataques cibernéticos y demás factores externos que incidan en la infraestructura.

d. **Grupos de trabajo y organizaciones asociadas:** Conformar grupos de trabajo que pueden incluir partes interesadas de una variedad de organizaciones tales como propietarios y operadores de instalaciones del sector privado, organizaciones de recuperación y respuesta a emergencias, proveedores de servicios públicos y autoridades reguladoras, agencias y autoridades de transporte, organizaciones de planificación metropolitana, organismos encargados de hacer cumplir la ley y de seguridad consejos tribales, instituciones académicas y centros de investigación, asociaciones industriales.

e. **Evaluaciones previas, planes, operativos y ejercicios:** Realizar evaluaciones en instalaciones ubicadas dentro del área de enfoque geográfico o la infraestructura de apoyo que tiene el potencial de proporcionar información sobre resiliencia; procesos de planificación colaborativa, lecciones aprendidas de los ejercicios de simulación.

f. **Análisis de peligros estatales y locales y evaluaciones de capacidades:** Se deben identificar las amenazas y evaluar los riegos externos e internos cada año, explorando qué amenazas y peligros pueden afectarlos, cuáles serían los impactos potenciales y qué capacidades deberían existir para gestionar eficazmente ese riesgo.

g. **Identificación de amenazas por parte de socios públicos y privados:** Se debe trabajar con centros de fusión como policía, seguridad pública, servicios de bomberos, respuesta a emergencias, etc, para la identificación de amenazas.

Paso 2. Diseño: En este paso se deben definir las preguntas clave de investigación que los esfuerzos de evaluación regional intentarán abordar, en este paso se establecen las 05 variables planteadas en la metodología acorde los siguientes ítems relevantes de estudio:

- Estableciendo la extensión geográfica del esfuerzo
- Identificando los sistemas de infraestructura que se considerarán en la evaluación
- Articulando los pasos específicos que las partes interesadas tomarán para abordar preguntas clave de investigación.
- Describir las características de la infraestructura existente.
- Definir infraestructura Cyber

Este paso es la base sobre la cual se crean las 05 variables para evaluar la ICC.

Paso 3. Recopilar datos: se aborda la investigación de fuentes, colaboración de varias agencias, entrevistas con expertos, discusiones, evaluaciones del sitio y otros pasos que ayudan a capturar la información necesaria para abordar las preguntas clave de investigación de la evaluación.

a. Métodos de recopilación: La revisión de literatura, investigación de fuentes abiertas -OSINT- (publicaciones en línea, blogs, redes sociales), medios (artículos de periódicos y revistas), datos públicos del gobierno (informes, discursos, sitios web, presentaciones de cumplimiento normativo), datos comerciales (informes de investigación de mercado empresarial, bases de datos), literatura gris (informes técnicos, patentes, libros blancos, trabajos no publicados, boletines, comunicados de prensa, presentaciones).

b. Otros Métodos: Entrevistas individuales, encuestas y evaluaciones estructuradas.

Paso 4. Analizar: En este enfoque se debe aplicar de un enfoque analítico para evaluar los sistemas de infraestructura de interés.

- Identificar las amenazas y peligros para la infraestructura.
- Evaluación de las vulnerabilidades de la infraestructura priorizada

- Evaluar las consecuencias y las interacciones entre los sistemas de infraestructura y priorizar el riesgo para los sistemas de infraestructura.
-

a. **Tipos de análisis que se pueden realizar durante la evaluación:** análisis de amenazas y peligros, análisis de vulnerabilidad, análisis de criticidad, análisis comparativo, análisis de planos, análisis geoespacial, análisis de capacidad, análisis de datos, análisis de red, análisis fallido, análisis de decisión. El análisis incluye la identificación de activos críticos, la cual se evalúa a la luz de las variables propuestas.

Paso 5. Documentar y entregar resultados: Acá se documentan los problemas específicos, retos y oportunidades descubiertas desde la evaluación y definición de potenciales cursos de acción que pueden comenzar a abordar las brechas de resiliencias identificadas.

Aquí, se agregan hallazgos importantes del análisis, se documentan los resultados e identifican cómo presentar la información para abordar con mayor eficacia el propósito original y los objetivos previstos resultados de la evaluación.

Se tiene en cuenta el desarrollo de cursos de acción, en donde se identifican los problemas de resiliencia y se visualizan posibles soluciones. Los cursos de acción bien construidos deben hacer lo siguiente:

- Identificar claramente las organizaciones que deberían liderar o tener un papel en su ejecución;

- Ser soluciones lógicas que sean relevantes para el problema identificado en el hallazgo clave;

- Ser factible de manera realista dentro de las limitaciones conocidas

- Identificar los recursos disponibles que pueden ayudar en su ejecución.

Los hallazgos clave de la evaluación y los cursos de acción, así como el cuerpo de investigación y análisis, deben presentarse a las partes interesadas en un formato convincente y útil (o múltiples formatos) que cumpla con los usos previstos, estos pueden ser:

- Informes narrativos que documentan análisis, hallazgos clave y recomendaciones.

- Listas de verificación que documentan vulnerabilidades a nivel de activos o sistemas y opciones para considerar mitigar esas vulnerabilidades.

- Sesiones informativas y presentaciones para entrega en reuniones interinstitucionales, talleres o industria / conferencias académicas.

- Infografías que representan datos y hallazgos.

- Productos cartográficos estáticos e interactivos que aprovechan los datos y análisis geoespaciales recopilados durante la evaluación para ilustrar hallazgos y

recomendaciones relevantes relacionados con sistemas de infraestructura regional.

- Herramientas de apoyo a la toma de decisiones que ayuda a las partes interesadas a probar posibles cursos de acción para tomar decisiones informadas (listas de verificación sencilla y árboles de decisión dentro de una interfaz de usuario simple u opciones de software más avanzadas que integran modelos y elementos de visualización).

- Los conjuntos de datos compilados como la información geoespacial, los resultados del modelado y los inventarios de activos que se recopilaron, seleccionaron o crearon durante el análisis de resiliencia, que también pueden proporcionar valor a las partes interesadas para una mayor planificación y análisis.

Paso 6. Promover la acción: Colocar el trabajo de base para la acción sobre los hallazgos analíticos y tomar medidas tangibles para mejorar la resiliencia a través de inversiones de capital, esfuerzos de planificación, capacitación y ejercicios.

En este punto es necesario implementar soluciones de resiliencia y medir su eficacia. Así se reconocen los elementos de infraestructura crítica:

a. **Tiene tres elementos:** físico, cibernético y humano.

b. **El intercambio de información entre estos elementos se da a través de los siguientes pasos:** fijar metas y objetivos; identificar la infraestructura; evaluar y analizar los riesgos; implementar riesgos de gestión y actividades; y, medidas de eficacia.

De tal forma, se cuenta con pasos específicos para mejorar la resiliencia regional de la infraestructura:

1. **Planeación:** Necesidad de desarrollar o actualizar planes, incluidos los planes estratégicos, operativos y tácticos.

2. **Inversiones de capital y presentaciones de subvenciones:** Los propietarios y operadores de instalaciones, las organizaciones regionales y las agencias gubernamentales pueden usar los hallazgos del análisis de resiliencia para guiar las inversiones estratégicas en equipo, planificación, capacitación y recursos para mejorar la resiliencia y la protección de las instalaciones, las comunidades circundantes y regiones enteras.

3. **Capacitación:** Estas necesidades de capacitación pueden incluir capacitación general sobre temas centrales (gestión de incidentes) o capacitación específica de la organización vinculada a políticas y procedimientos (garantizar que el personal conozca la continuidad del negocio o el plan de operaciones de emergencia).

4. **Ejercicios:** Medio para explotar más a fondo los riesgos recién identificados, resolver las brechas de coordinación y planificación, y diseñar enfoques para otros problemas de infraestructura identificados durante el curso de una resiliencia de evaluación regional.

- Es de destacar que, uno de los principales desafíos para la resiliencia de la infraestructura es la creciente complejidad de la infraestructura de moderna actual. La infraestructura está conectada a muchos otros activos, sistemas y redes de infraestructura de los que dependen para las operaciones normales del día a día.

6. Conceptos de evaluación o variable para la identificación de infraestructuras críticas cibernética nacional

Colombia con este documento busca actualizar la metodología de identificación de infraestructura crítica cibernética, con base en el decreto 338, el cual insta a identificar infraestructuras críticas y de un sistema unificado de evaluación y seguimiento a esta.

Por lo que la identificación de IC a nivel nacional se ha basado en procedimientos particulares que cada entidad pública y particular ha construido de acuerdo con sus necesidades y funciones. Donde se destacan tres variables fundamentales: a) Sociales, que analizan el impacto de la IC en la calidad de vida de la población; b) Económicas, que analizan el impacto de la IC en la economía nacional y departamental; y c) Medioambientales, que analizan el impacto de la IC en la biodiversidad y los recursos ecosistémicos.

Si bien, estas variables han permitido identificar y evaluar las infraestructuras y activos críticos a nivel nacional, en un contexto cada vez más complejo y cambiante gracias a la interconexión global por el crecimiento acelerado de las TIC, se hace necesario actualizar el enfoque de identificación de infraestructuras críticas para hacer frente a nuevos riesgos y amenazas. Incorporando nuevas variables que permitan una identificación más precisa y completa de las infraestructuras críticas en Colombia para luego, poder pasar a la identificación de una Infraestructura crítica cibernética, la cual se encuentra definida en el Decreto Único 1078 de 2015 adicionado por el Decreto 338 de 2022, como aquellos *"Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía"*.

En esta última sección se propone una metodología para identificar las infraestructuras críticas públicas cibernéticas nacionales y de servicios esenciales, considerando metodologías internacionales y las infraestructuras críticas de países referentes en ciberseguridad. Proponiendo a partir de este estudio comparativo 5 variables nuevas o conceptos de evaluación para la identificación de infraestructuras críticas cibernéticas en Colombia. Estos son los siguientes, los cuales se exponen de manera general y se anexan un archivo en Excel con la definición de cada una de ellas.

1. **Impacto a las funciones críticas nacionales:** Esta variable evalúa el impacto sobre cuantas funciones críticas nacionales se ven afectadas por la afectación de la seguridad del activo de infraestructura crítica cibernética. Lo anterior, con base en las categorías de comunicación, distribución, administración y suministro.

2. **Contexto y/o población afectada:** Esta variable se refiere al contexto y la importancia del sistema, incluyendo la cantidad de personas que se perturba en el servicio de una infraestructura crítica, y a la densidad poblacional en la zona de influencia de dicha infraestructura, lo anterior con un enfoque de Derechos Humanos, por lo que es esencial que en esta variable se evalúa el impacto sobre su afectación. Esta variable es importante para evaluar el grado

de impacto en la población y la necesidad de priorizar la recuperación del servicio.

3. **Impacto operacional:** Esta variable mide el impacto y alcance en el funcionamiento, teniendo en cuenta la salud pública, área geográfica, entre otros, que se vería afectada en caso de interrupción del servicio de una infraestructura crítica. Se consideran aspectos como la cantidad de usuarios y la distribución geográfica de la infraestructura. Evaluar esta variable es importante porque permite identificar las zonas más vulnerables y establecer planes de **contingencia** que aborden específicamente el impacto en cada área geográfica afectada.

   En esta variable es fundamental trabajar de la mano con otros departamentos gubernamentales encargados de estudiar factores que tienen un impacto operacional en la IC. Por ejemplo, en el caso de determinar las dependencias geográficas se deben tener en cuenta los informes de entidades encargadas de estudiar los fenómenos climáticos como lo es el IDEAM y el Banco de la República[19]

4. **Afectación Económica Nacional:** Esta variable mide el impacto que la interrupción del servicio de una infraestructura crítica tendría sobre la economía del país, específicamente sobre el Producto Interno Bruto (PIB). Se consideran aspectos como la disminución en la producción, la pérdida de empleos y la reducción en las exportaciones. Esto es una estimación con base en los datos que provee el DANE.

5. **Impacto Nacional al servicio:** Impacto Nacional del Servicio - Incidentes que podrían afectar al servicio del Estado, esto pensado en términos de seguridad nacional, derechos humanos y la afectación correlacionada otros sectores esenciales o con los que se tenga relación. Impacto de su servicio y la interdependencia con otro sector

14. Definición de las variables y explicación en la metodología:

Las Infraestructuras Críticas Cibernéticas en la metodología se organizan en sectores y se procura por lograr identificar los subsectores y los operadores, de manera escalonada. Lo anterior, ya que pueden representar cada uno una categoría general de servicios y sistemas esenciales.

En ese sentido se propone:

[19] Banco de la República. (2023). Desastres naturales en Colombia: un análisis regional. Señala que, Colombia por su ubicación geográfica es uno de los países en Latinoamérica más propensos a sufrir desastres naturales, siendo los departamentos de Antioquia y Putumayo los que sufrieron un mayor número de pérdidas humanas por desastres naturales.

Paso 1. Teniendo en cuenta la identificación de activos críticos de información de su entidad según el Modelo de Privacidad y Seguridad de la Información (MSPI). El cual debe tener cada entidad.

Paso 2. Con base en el paso 1 desarrolle la matriz en Excel con los factores de evaluación y la delimitación de la infraestructura crítica cibernética (anexo número 1).

Paso 3. Seguimiento y control de las ICC (anexo número 2).

6.1.1 Definición de variables

- Activos - Serían los elementos tangibles o intangibles que son esenciales para que los sistemas funcionen.

- Indicador o Clasificación de Incidentes - Etiquetará los sucesos en función de su gravedad y/o impacto potencial en sus sectores.

En el caso de la metodología en Colombia se utilizará la taxonomía de clasificación de incidentes de COLCERT[20], en esta parte se debe especificar el tipo de clasificación o potencial incidente sobre el activo.

La escala de evaluación se alinea a guía de DAFP (1) Bajo; (2) Moderado; (3) alto ; (4) Extremo.

A. FUNCIONES CRÍTICAS NACIONALES: Se define como LA FUNCIÓN CRÍTICA DEL ESTADO, Esto tendría consecuencias para los roles esenciales de la ICC en un mayor número de las Funciones Críticas Nacionales.

La escala de evaluación se alinea a guía de DAFP se define así:

• Bajo (1) = Impacto una o ninguna función crítica nacional que afecte su servicio.

• Moderado (2) = Supone un impacto potencial en dos funciones críticas Nacionales con impacto en su organización y otros sectores de apoyo.

• Alto (3) = Tendrá un impacto en tres funciones críticas nacionales, es probable que afecte a otras organizaciones.

• Extremo (4) = Tendrá un impacto grave en 04 o más funciones críticas nacionales, lo que se refleja en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas funciones se dividen en 04 grandes categorías y cada una de ellas incluye cada una de las funciones de la siguiente manera: [21]

[20] https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

[21] Definición de funciones críticas nacionales adaptadas de https://www.rand.org/pubs/research_reports/RRA1512-1.html

Conexión Comunicación	Distribución	Administración	Suministro
1. Operación del Core Network (Núcleo de la red operada)	1. Distribución de electricidad	1. Celebración de elecciones	1. Exploración y extracción de combustibles
2. Prestación de servicios de redes de acceso por cable o redes alámbricas.	2. Mantener las cadenas de suministro	2. Desarrollar y mantener obras y servicios públicos	2. Refinación y procesamiento de combustibles
3. Prestación de servicios de comunicación e información de contenidos basados en Internet	3. Transmisión de electricidad	3. Educación y formación	3. Generación de electricidad
4. Prestación de servicios de enrutamiento, acceso y conexión a Internet	4. Transportar carga y pasajeros por aire	4. Cumplimiento de la ley/normatividad (Law Enforcement)	4. Manufactura de equipos/materiales /insumos
5. Prestación de servicios de posicionamiento, navegación y tiempo.	5. Transportar carga y pasajeros por ferrocarril	5. Mantener el acceso a los historiales médicos	5. Producción y suministro de productos y servicios agrícolas
6. Prestación de servicios de redes de acceso de radiodifusión	6. Transportar carga y pasajeros por carretera	6. Gestionar los materiales peligrosos	6. Producción y suministro de productos y servicios de alimentación humana y animal
7. Prestación de servicios de redes de acceso por satélite	7. Transportar carga y pasajeros por barco	7. Gestionar las aguas residuales	7. Producción de productos químicos

Conexión Comunicación	Distribución	Administración	Suministro
8. Prestación de servicios de redes de acceso inalámbricas	8. Transportar materiales por ductos, oleoductos o gasoductos.	8. Gestionar la administración pública	8. Suministro de metales y materiales
	10. Transporte masivo de pasajeros	9. Disponer de capacidades de gestión de incidentes cibernéticos	9. Suministro de viviendas
		10. Prepararse para las emergencias y gestionarlas	10. Suministro de productos y servicios de tecnología de la información
		11. Preservar los derechos constitucionales	11. Suministro de material y apoyo operativo a la defensa
		12. Proteger la información confidencial	12. Investigación y desarrollo
		13. Proporcionar y mantener infraestructuras (Física)	13. Suministro de agua
		14. Prestar servicios de mercados de capitales y actividades de inversión	
		15. Prestar servicios de banca comercial y de consumo	
		16. Prestar servicios de financiación y liquidez	
		17. Prestar servicios de gestión de identidad y servicios de apoyo fiduciario asociados	

Conexión Comunicación	Distribución	Administración	Suministro
		18. Prestar servicios de seguros	
		19. Prestar asistencia médica	
		20. Prestar servicios de compensación y liquidación de pagos	
		21. Proporcionar seguridad pública	
		22. Proporcionar financiación mayorista	
		23. Almacenar combustible y mantener reservas	
		24. Apoyar la salud de la comunidad	

B. Contexto/Población - Se basaría en la población afectada por la interrupción del sector. En esta variable se tiene en cuenta la afectación a los derechos humanos. La escala de esta se define con base en el método Hanlon, el cual es una herramienta utilizada en el campo de la salud pública para priorizar problemas de salud y asignar recursos de manera efectiva. En ese sentido, se toma el componente de magnitud para entender el número de personas afectadas por el problema en relación con la población total. El cual se basa en una estimación a partir de Hanlon, J.J. y Pickent, George E. Public Health Administration and Practice. Ed 8.

- Bajo (1) = 99.999 o menos personas
- Moderado (2) = de 100.000 a 249.999 personas
- Alto (3) = de 250.000 a 499.999 persona
- Extremo (4) =Impacto potencial a 500. 000 o más personas

C. Impacto Operacional

Esta variable mide el impacto y alcance en el funcionamiento (servicios de la entidad, teniendo en cuenta la salud pública, área geográfica, entre otros, que se vería afectada en

caso de interrupción del servicio de una infraestructura crítica. Se consideran aspectos como la cantidad de usuarios y la distribución geográfica de la infraestructura.

Bajo (1) = Nivel menor: El impacto que causa la materialización del riesgo en los objetivos de la entidad es mínimo. El impacto de la operación es pequeño en el territorio o la entidad.

Moderado (2) = Nivel moderado: La materialización del riesgo puede causar una pérdida momentánea. El impacto afecta momentáneamente pero breve la operación de la entidad y/o en los territorios.

Alto (3) = Nivel mayor: Genera retrasos importantes que afectan el cumplimiento de los objetivos. En esta parte se afecta la operación de la entidad y sus acciones en el territorio.

Extremo (4) = Nivel catastrófico: Puede detener la operación de la entidad, incluso, tener consecuencias como el cierre definitivo. Afecta la operación total de la entidad y su despliegue en territorio.

D. Afectación Económica Nacional

La afectación Económica nacional mide el impacto de un incidente económico en términos del PIB, tomando en cuenta lo siguiente:

Bajo (1) =Impacto menor al 0,1% del PIB

Moderado (2) = Impacto inferior del 0,1 al 0,5%

Alto (3) = Impacto del 0,5 al 1% del PIB.

Extremo (4) = Impacto mayor al 1% del PIB.

Lo que se mide de la siguiente manera:

Impacto económico en porcentaje del PIB = (Valor del impacto económico / PIB) * 100

El impacto se mide según los siguientes datos:

- PIB Colombia año 2023: 1,572,459.000.000
- Este valor se debe dividir sobre el valor del impacto[22] económico del sector/PIB *100.

Los datos del PIB enfoque de la producción se toman del DANE, en la tabla que se adjunta.

E. Impacto Nacional del Servicio: Incidentes que podrían afectar al servicio del Estado y otros sectores esenciales o con los que se tenga relación. Impacto de su servicio y la interdependencia con otro sector

Ejemplos:

• Interrupciones

• Tiempo de inactividad

• Averías de equipos

[22] El valor del impacto económico se entrega acorde a la proyección del DANE por sectores

• Problemas de seguridad/catástrofes naturales

• Pérdida de control

• Bajo (1) = Impacto muy bajo en la organización, improbable que afecte a otras organizaciones

• Moderado (2) = Supone un impacto potencial para la organización, posibilidad mínima de impacto para otras organizaciones

• Alto (3) = Tendrá un impacto en la organización, es probable que afecte a otras organizaciones

• Extremo (4) = Tendrá un impacto grave en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas son las 05 variables que se evalúan junto a esta se establece el tiempo de indisponibilidad y recuperación acorde a la siguiente escala:

Escala

Bajo (1) =. El tiempo de indisponibilidad del activo es de 24 horas o menos.

Moderado (2) = El tiempo de indisponibilidad del activo es de 24 a 72 horas.

Alto (3) = El tiempo de indisponibilidad del activo es de 72 horas a una semana.

Extremo (4) = El tiempo de indisponibilidad del activo es superior a una semana o no se puede determinar por su alto impacto

DELIMITACIÓN INFRAESTRUCTURA CRÍTICA CIBERNÉTICA													
Sectores	Gobierno/Estado								Comentarios:		Entidades adscritas que hacen parte del sector		
Sub sector	Gasto												
Relación o sector de apoyo													
Actividad esencial/Servicios prestados	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Activos Cibernético	Escenario de pilar de la información afectado	Riesgo (tipo de incidente)	Tiempo de indisponibilidad	Impacto en las Funciones Críticas Nacionales	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
Contratación pública del Estado	Administración	8. Gestionar la administración pública	Portal Web	Disponibilidad	3. DoS (Denegación de Servicio): Ataques que buscan hacer que un servicio no esté disponible.	1	1	1	4	3	4	1	2,29
Contratación pública del Estado	Administración	1. Celebración de elecciones	Base de datos	Integridad	3. Pérdida de datos: Puede resultar en la corrupción o eliminación de información.	2	1	4	4	3	4	2	3,00
Gestión de proyectos de inversión	Suministro		Plataforma gestión pública			2	4	4	4	1	4	2	3,17

Ilustración 4 Paso 3 identificación de ICC

Resultado de la evaluación se presenta la escala de las categorías y definiciones de Infraestructura crítica cibernética/ Servicios esenciales:

1. La ICC todo lo que en la evaluación de entre 2,45 a 4. (Categoría Crítico) - Extremo

2. Servicio Esencial: todo aquel que en la escala se encuentre entre 1,95 y 2,94. (Categoría Esencial) - Alto

3. Servicio no esencial, pero con impacto a la seguridad: todo entre 0.95 y 1.94. (Categoría importante) - Moderado

4. Activo que se contempla, pero no cumple un impacto a nivel nacional. – (Categoría Secundario) - Bajo

15. Actualización en la metodología:

En la propuesta se menciona modificar las variables de estudio para evaluar sectores y subsectores, en ese sentido, se modifica el punto número 5. En el que se amplía las tres variables y se propone el estudio de impacto a partir de las mencionadas.

A su vez, la propuesta va encaminada a:

- Incluir la sección de etiquetado para ICC (Infraestructura Crítica Cibernética).
- Actualizar la clasificación de activos.
- Establecer un capítulo con la descripción de los criterios de identificación.
- Definir operadores de las infraestructuras Críticas Cibernéticas y las redes de operación.
- Incluir, Interdependencias:

- Internas entre subsectores o servicios de un mismo sector

-Entre sectores críticos

-Entre activos de la red de datos de varios sectores.

- Ajustar el formato de identificación y clasificación de activos para ICC manejando únicamente lo relacionado con seguridad digital (una vez ya se haya identificado los activos de información).
- Identificar los activos de criticidad alta y media e incluir criterios de identificación de ICC para ellos.
- Actualizar anexo 4 Guía para la gestión del riesgo y diseño de controles a través de la identificación de activos de información y el reporte de la gestión del riesgo de seguridad de la información autoridades o entidades especiales asociada al MSPI.

Consideraciones finales

Con estos lineamientos se consolidan los criterios mínimos para el reporte de información por parte de las entidades públicas y se busca servir como referente frente a las entidades privadas.

La metodología para la identificación de las Infraestructuras Críticas Cibernéticas tiene por objeto ayudar a los propietarios y operadores a identificación de Infraestructuras Críticas, evaluar cualquier riesgo relacionado, y desarrollar e implementar soluciones de resiliencia.

Las infraestructuras críticas cibernéticas pueden ser propiedad y estar gestionadas por una amplia gama de entidades de los sectores público y privado. Estos lineamientos ayudarán a dirigir y alinear los diversos esfuerzos relacionados con la seguridad y la resistencia de estos sistemas, aunque no hay dos sistemas iguales, esta estrategia pretende sentar las bases para la identificación de Infraestructuras cibernéticas.

La Infraestructura Crítica incluye servicios tales como activos, sistemas, instalaciones, redes y otros sistemas vitales de los que la sociedad colombiana depende para mantener la economía, la salud pública, la seguridad y varias Funciones Críticas Nacionales para mantener al país "funcionando". La Infraestructura Crítica puede definirse mejor como aquellos sistemas y activos, ya sean físicos o virtuales que son tan vitales que su incapacidad o destrucción puede tener un impacto debilitante en la seguridad, la economía, la salud pública o la seguridad de la nación, la salud pública o la seguridad de la nación.

16. Orientación

1. Identificar la ICC, ser capaz de identificar los problemas que los sectores específicos

deben abordar y desarrollar un concepto que pueda ejecutarse conjuntamente.

2. Diseñar la evaluación con preguntas claves de investigación que permitan realizar una evaluación eficaz en territorio.

3. Recopilación de datos, llevar a cabo la investigación, recopilación multiinstitucional, entrevistas con expertos en la materia, debates facilitados, evaluaciones in situ y otros pasos que ayuden a las partes interesadas a recopilar la información abordar las preguntas clave de investigación de la evaluación.

4. Analizar y utilizar diversas técnicas analíticas para evaluar los sistemas de interés.

5. Documentar y entregar resultados para proporcionar una documentación escrita de los problemas, retos y oportunidades descubiertos a partir de la evaluación y la definición de posibles líneas de acción que puedan empezar a abordar las deficiencias de resiliencia identificadas

6. Promover la acción a realizar sobre los resultados analíticos y tomar medidas tangibles para mejorar resiliencia mediante inversiones de capital, esfuerzos de planificación, formación y ejercicios.

Paso a paso para la identificación de las ICC

En un mundo dinámico e interconectado, donde la privacidad y la seguridad de los datos es fundamental, surge la protección de infraestructuras críticas cibernéticas como un eje esencial para garantizar la continuidad y la seguridad de los servicios fundamentales, teniendo en cuenta la garantía de los derechos humanos y la protección de los derechos fundamentales.

Las infraestructuras Criticas Cibernéticas abarcan los 13 sectores, desde energía y transporte hasta redes de comunicación, son vulnerables a las amenazas cibernéticas que pueden afectar gravemente la seguridad, estabilidad social, económica y política de un país.

Este paso a paso tiene como objetivo guiar el proceso de levantamiento de infraestructuras críticas cibernéticas, el cual se enfoca en tres etapas clave: la **identificación de activos**

críticos, la **evaluación mediante una matriz de variables que contempla, evaluar los activos críticos, frente a las actividades y servicios prestados, a la luz de evaluar escenarios frente a:**

1. Impacto en las funciones críticas nacionales
2. Contexto y/o población afectada
3. Impacto operacional
4. Afectación económica nacional
5. Impacto nacional del servicio

- Tiempo de recuperación de activo planteado en la guía de riesgos.

y la implementación de un **control de seguimiento y gestión de riesgos**. A través de este enfoque estructurado, las organizaciones pueden identificar la infraestructura crítica cibernética, los servicios esenciales, las vulnerabilidades, priorizar recursos de protección y establecer mecanismos proactivos y de anticipación para mitigar riesgos, garantizando así la resiliencia y seguridad de sus infraestructuras críticas.

Las Infraestructuras Críticas Cibernéticas se identificarán inicialmente en los 13 sectores establecidos en el documento matriz, paulatinamente se procurará lograr identificar los subsectores y los operadores de manera escalonada. Lo anterior, ya que cada uno puede representar una categoría general de servicios y sistemas esenciales.

En ese sentido se propone:

Paso 1. Identifique los activos críticos de información de su entidad según el Modelo de Privacidad y Seguridad de la Información (MSPI).

Paso 2. Aplique los controles correspondientes según la guía de gestión de riesgos asociada al MSPI.

Paso 3. Con base en el paso 1 y 2 diligencie la matriz en formato Excel con los factores de evaluación y la delimitación de la infraestructura crítica cibernética (anexo número 1).

Paso 4. Seguimiento y control de las ICC (anexo número 2).

Definición de variables

- Activos - Serían los elementos tangibles o intangibles que son esenciales para que los sistemas funcionen.

- Indicador o Clasificación de Incidentes - Etiquetará los sucesos en función de su gravedad y/o impacto potencial en sus sectores.

En el caso de la metodología en Colombia se utilizará la taxonomía de clasificación de incidentes de COLCERT[23], en esta parte se debe especificar el tipo de clasificación o potencial incidente sobre el activo.

La escala de evaluación se alinea a guía de DAFP (1) Bajo; (2) Moderado; (3) alto; (4) Extremo.

[23] https://www.colcert.gov.co/800/articles-198656_taxonomia.pdf

A. IMPACTO A LA SEGURIDAD: Se define como LA FUNCIÓN CRÍTICA DEL ESTADO, Esto tendría consecuencias para los roles esenciales de la ICC en un mayor número de las Funciones Críticas Nacionales.

La escala de evaluación se alinea a guía de DAFP se define así:

• Bajo (1) = Impacto una o ninguna función crítica nacional que afecte su servicio.

• Moderado (2) = Supone un impacto potencial en dos funciones críticas Nacionales con impacto en su organización y otros sectores de apoyo.

• Alto (3) = Tendrá un impacto en tres funciones críticas nacionales, es probable que afecte a otras organizaciones.

• Extremo (4) = Tendrá un impacto grave en 04 o más funciones críticas nacionales, lo que se refleja en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas funciones se dividen en 04 grandes categorías y cada una de ellas incluye cada una de las funciones de la siguiente manera: [24]

Conexión Comunicación	Distribución	Administración	Suministro
1. Operación del Core Network (Núcleo de la red operada)	1. Distribución de electricidad	1. Celebración de elecciones	1. Exploración y extracción de combustibles
2. Prestación de servicios de redes de acceso por cable o redes alámbricas.	2. Mantener las cadenas de suministro	2. Desarrollar y mantener obras y servicios públicos	2. Refinación y procesamiento de combustibles
3. Prestación de servicios de comunicación e información de contenidos basados en Internet	3. Transmisión de electricidad	3. Educación y formación	3. Generación de electricidad
4. Prestación de servicios de enrutamiento, acceso y	4. Transportar carga y pasajeros por aire	4. Cumplimiento de la ley/normatividad (Law Enforcement)	4. Manufactura de equipos/materiales /insumos

[24] Definición de funciones críticas nacionales adaptadas de https://www.rand.org/pubs/research_reports/RRA1512-1.html

Conexión Comunicación	Distribución	Administración	Suministro
conexión a Internet			
5. Prestación de servicios de posicionamiento, navegación y tiempo.	5. Transportar carga y pasajeros por ferrocarril	5. Mantener el acceso a los historiales médicos	5. Producción y suministro de productos y servicios agrícolas
6. Prestación de servicios de redes de acceso de radiodifusión	6. Transportar carga y pasajeros por carretera	6. Gestionar los materiales peligrosos	6. Producción y suministro de productos y servicios de alimentación humana y animal
7. Prestación de servicios de redes de acceso por satélite	7. Transportar carga y pasajeros por barco	7. Gestionar las aguas residuales	7. Producción de productos químicos
8. Prestación de servicios de redes de acceso inalámbricas	8. Transportar materiales por ductos, oleoductos o gasoductos.	8. Gestionar la administración pública	8. Suministro de metales y materiales
	10. Transporte masivo de pasajeros	9. Disponer de capacidades de gestión de incidentes cibernéticos	9. Suministro de viviendas
		10. Prepararse para las emergencias y gestionarlas	10. Suministro de productos y servicios de tecnología de la información
		11. Preservar los derechos constitucionales	11. Suministro de material y apoyo operativo a la defensa
		12. Proteger la información confidencial	12. Investigación y desarrollo

Conexión Comunicación	Distribución	Administración	Suministro
		13. Proporcionar y mantener infraestructuras (Física)	13. Suministro de agua
		14. Prestar servicios de mercados de capitales y actividades de inversión	
		15. Prestar servicios de banca comercial y de consumo	
		16. Prestar servicios de financiación y liquidez	
		17. Prestar servicios de gestión de identidad y servicios de apoyo fiduciario asociados	
		18. Prestar servicios de seguros	
		19. Prestar asistencia médica	
		20. Prestar servicios de compensación y liquidación de pagos	
		21. Proporcionar seguridad pública	
		22. Proporcionar financiación mayorista	
		23. Almacenar combustible y mantener reservas	

Conexión Comunicación	Distribución	Administración	Suministro
		24. Apoyar la salud de la comunidad	

B. Contexto/Población - Se basaría en la población afectada por la interrupción del sector. La escala de esta se define con base en el método Hanlon, el cual es una herramienta utilizada en el campo de la salud pública para priorizar problemas de salud y asignar recursos de manera efectiva. En ese sentido, se toma el componente de magnitud para entender el número de personas afectadas por el problema en relación con la población total. El cual se basa en una estimación a partir de Hanlon, J.J. y Pickent, George E. Public Health Administration and Practice. Ed 8.

- Bajo (1) = 99.999 o menos personas
- Moderado (2) = de 100.000 a 249.999 personas
- Alto (3) = de 250.000 a 499.999 persona
- Extremo (4) =Impacto potencial a 500. 000 o más personas

C. Impacto Operacional

Esta variable mide el impacto y alcance en el funcionamiento (servicios de la entidad, teniendo en cuenta la salud pública, área geográfica, entre otros, que se vería afectada en caso de interrupción del servicio de una infraestructura crítica. Se consideran aspectos como la cantidad de usuarios y la distribución geográfica de la infraestructura.

Bajo (1) = Nivel menor: El impacto que causa la materialización del riesgo en los objetivos de la entidad es mínimo. El impacto de la operación es pequeño en el territorio o la entidad.

Moderado (2) = Nivel moderado: La materialización del riesgo puede causar una pérdida momentánea. El impacto afecta momentáneamente pero breve la operación de la entidad y/o en los territorios.

Alto (3) = Nivel mayor: Genera retrasos importantes que afectan el cumplimiento de los objetivos. En esta parte se afecta la operación de la entidad y sus acciones en el territorio.

Extremo (4) = Nivel catastrófico: Puede detener la operación de la entidad, incluso, tener consecuencias como el cierre definitivo. Afecta la operación total de la entidad y su despliegue en territorio.

D. Afectación Económica Nacional

La afectación Económica nacional mide el impacto de un incidente económico en términos del PIB, tomando en cuenta lo siguiente:

Bajo (1) =Impacto menor al 0,1% del PIB

Moderado (2) = Impacto inferior del 0,1 al 0,5%

Alto (3) = Impacto del 0,5 al 1% del PIB.

Extremo (4) = Impacto mayor al 1% del PIB.

Lo que se mide de la siguiente manera:

Impacto económico en porcentaje del PIB = (Valor del impacto económico / PIB) * 100

El impacto se mide según los siguientes datos:

- PIB Colombia año 2023: 1,572,459.000.000
- Este valor se debe dividir sobre el valor del impacto[25] económico del sector/PIB *100.

Los datos del PIB enfoque de la producción se toman del DANE, en la tabla que se adjunta.

E. Impacto Nacional del Servicio: Incidentes que podrían afectar al servicio del Estado y otros sectores esenciales o con los que se tenga relación. Impacto de su servicio y la interdependencia con otro sector

Ejemplos:

• Interrupciones

• Tiempo de inactividad

• Averías de equipos

• Problemas de seguridad/catástrofes naturales

• Pérdida de control

• Bajo (1) = Impacto muy bajo en la organización, improbable que afecte a otras organizaciones

• Moderado (2) = Supone un impacto potencial para la organización, posibilidad mínima de impacto para otras organizaciones

• Alto (3) = Tendrá un impacto en la organización, es probable que afecte a otras organizaciones

• Extremo (4) = Tendrá un impacto grave en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

Estas son las 05 variables que se evalúan junto a esta se establece el tiempo de indisponibilidad y recuperación acorde a la siguiente escala:

Escala

Bajo (1) =. El tiempo de indisponibilidad del activo es de 24 horas o menos.

Moderado (2) = El tiempo de indisponibilidad del activo es de 24 a 72 horas.

Alto (3) = El tiempo de indisponibilidad del activo es de 72 horas a una semana.

Extremo (4) = El tiempo de indisponibilidad del activo es superior a una semana o no se puede determinar por su alto impacto

[25] El valor del impacto económico se entrega acorde a la proyección del DANE por sectores

DELIMITACIÓN INFRAESTRUCTURA CRÍTICA CIBERNÉTICA										
Sectores	Gobierno/Estado					Comentarios		Entidades adscritas que hacen parte del sector		
Sub sector	Gasto									
Relación o sector de apoyo										
Actividad escenecial/Servicios prestados	Activos	Clasificación de incidente (tipo de incidente)	Tiempo de indisponibilidad	Impacto a la seguridad	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
Contratación pública del Estado	Portal Web	DoS (Denegación de Servicio)	1	4	1	4	3	4	1	2.83
Contratación pública del Estado	Base de datos	Phishing	2	4	4	4	3	4	2	3.50
Gestión de proyectos de inversión	Plataforma gestión pública	APT	2	4	4	4	1	4	2	3.17

Ilustración 4 Paso 3 identificación de ICC

Resultado de la evaluación se presenta la escala de las categorías y definiciones de Infraestructura crítica cibernética/ Servicios esenciales:

1. La ICC todo lo que en la evaluación de entre 2,45 a 4. (Categoría Crítico) - Extremo

2. Servicio Esencial: todo aquel que en la escala se encuentre entre 1,95 y 2,94. (Categoría Esencial) - Alto

3. Servicio no esencial, pero con impacto a la seguridad: todo entre 0.95 y 1.94. (Categoría importante) - Moderado

4. Activo que se contempla, pero no cumple un impacto a nivel nacional. – (Categoría Secundario) - Bajo

Importante:

Una vez, se diligencie la matriz en el formato Excel, la entidad representante de cada sector deberá diligenciar el anexo 2. *Estado actual de la infraestructura crítica cibernética de cada organización.* En el siguiente Link: https://forms.office.com/r/bvYF1QCBUF .

Posteriormente, deberá remitir al correo icc@colcert.gov.co la información que se encuentra en color verde, junto con el anexo 2 diligenciado y deberá ocultar la demás información con el fin asegurar su confidencialidad.

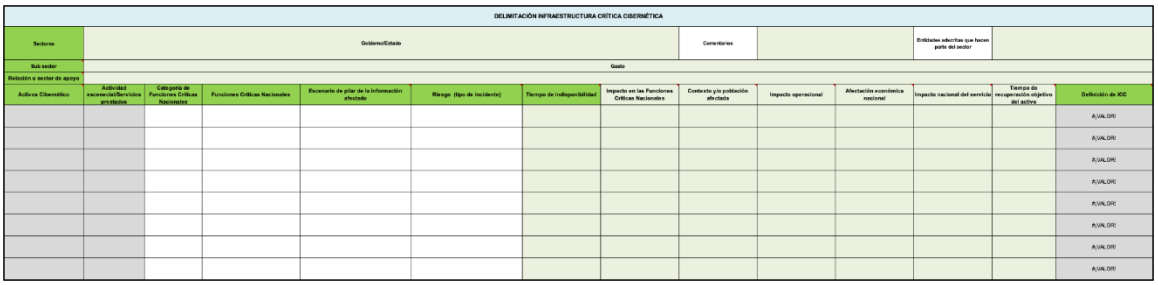
17. Fuentes

1. Catálogo de ICC, 2019, Consejo Privado de Competitividad, https://compite.com.co/wp-content/uploads/2019/06/ICC_2019_V1_VWeb.pdf
2. Cybersecurity and Crítical Infrastructure, 2020, Homeland Security, https://www.dhs.gov/archive/coronavirus/cybersecurity-and-crítical-infrastructure
3. Information Technology Sector-Specific Plan: An Annex to the NIPP 2013, 2016, Homeland Security, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf
4. Public Summary of Sector Security and Resilience Plans, 2018, Cabinet Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
5. Methodologies for the identification of Crítical Information Infrastructure assets and services, 2015, ENISA, https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis
6. National Strategy for Crítical Infrastructure, 2009, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
7. Artículo 333, 1991, Constitución Política de Colombia, https://www.constitucioncolombia.com/titulo-12/capitulo-1/articulo-333
8. Artículo 365, 1991, Constitución Política de Colombia, https://www.constitucioncolombia.com/titulo-12/capitulo-5/articulo-365
9. Ley 1341, 2009, Congreso de Colombia, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913
10. Decreto 338, 2022, Ministerio de Tecnologías de la Información y las Comunicaciones, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866
11. OECD Reviews of Risk Management Policies, Good Governance for Crítical Infrastructure Resilience, 2019, OECD iLibrary, https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en
12. Analysis of Crítical Infrastructure Dependencies and Interdependencies, 2015, Argonne National Laboratory, https://publications.anl.gov/anlpubs/2015/06/111906.pdf
13. National Strategy for Crítical Infrastructure, 2009, Public Safety Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf
14. Framework for Improving Crítical Infrastructure Cybersecurity, 2018, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
15. Crítical Infrastructure Resilience Strategy, 2023, Cyber and Infrastructure Security Centre, https://www.tisn.gov.au/Documents/Australian+Government+s+Crítical+Infrastructure+Resilience+Strategy.pdf
16. Good Governance for Crítical Infrastructure Resilience, 2019, OECD, https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/swissbasicstrategyforcríticalinfrastructureprotecti on.htm

17. Information Technology Sector-Specific Plan: An Annex to the NIPP 2013, 2016, Homeland Security, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf
18. Public Summary of Sector and Resilience Plans, 2018, Cabinet Office, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
19. RAND Corporation. (2023). *Identifying and Prioritizing Systemically Important Entities*. https://www.rand.org/pubs/research_reports/RRA1512-1.html

18. ANEXOS:

Anexo 1. Delimitación de sectores (Matriz en formato Excel).



DELIMITACIÓN INFRAESTRUCTURA CRÍTICA CIBERNÉTICA

Sectores	Gobierno/Estado			Comentarios		Entidades adscritas que hacen parte del sector	
Sub sector	Gasto						
Relación o sector de apoyo							

Activos Cibernético	Actividad escencial/Servicios prestados	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Escenario de pilar de la información afectado	Riesgo (tipo de incidente)	Tiempo de indisponibilidad	Impacto en las Funciones Críticas Nacionales	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!
													#¡VALOR!

Impacto en las Funciones Críticas Nacionales	Contexto y/o población afectada	Impacto operacional	Afectación económica nacional	Impacto nacional del servicio	Tiempo de recuperación objetivo del activo	Definición de ICC
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!
						#¡VALOR!

Activos Cibernético	Actividad escenecial/Servicios prestados	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Escenario de pilar de la información afectado	Riesgo (tipo de incidente)	Tiempo de indisponibilidad

Anexo 2. Estado actual de la infraestructura crítica cibernética de cada organización. (Actualizable cada año) https://forms.office.com/r/bvYF1QCBUF