



TIC





TIC



Lineamientos para la identificación de Infraestructuras Críticas Cibernéticas

www.mintic.gov.co



COLCERT

TLP:CLEAR

Antecedentes de las Infraestructuras Críticas y su metodología en Colombia.



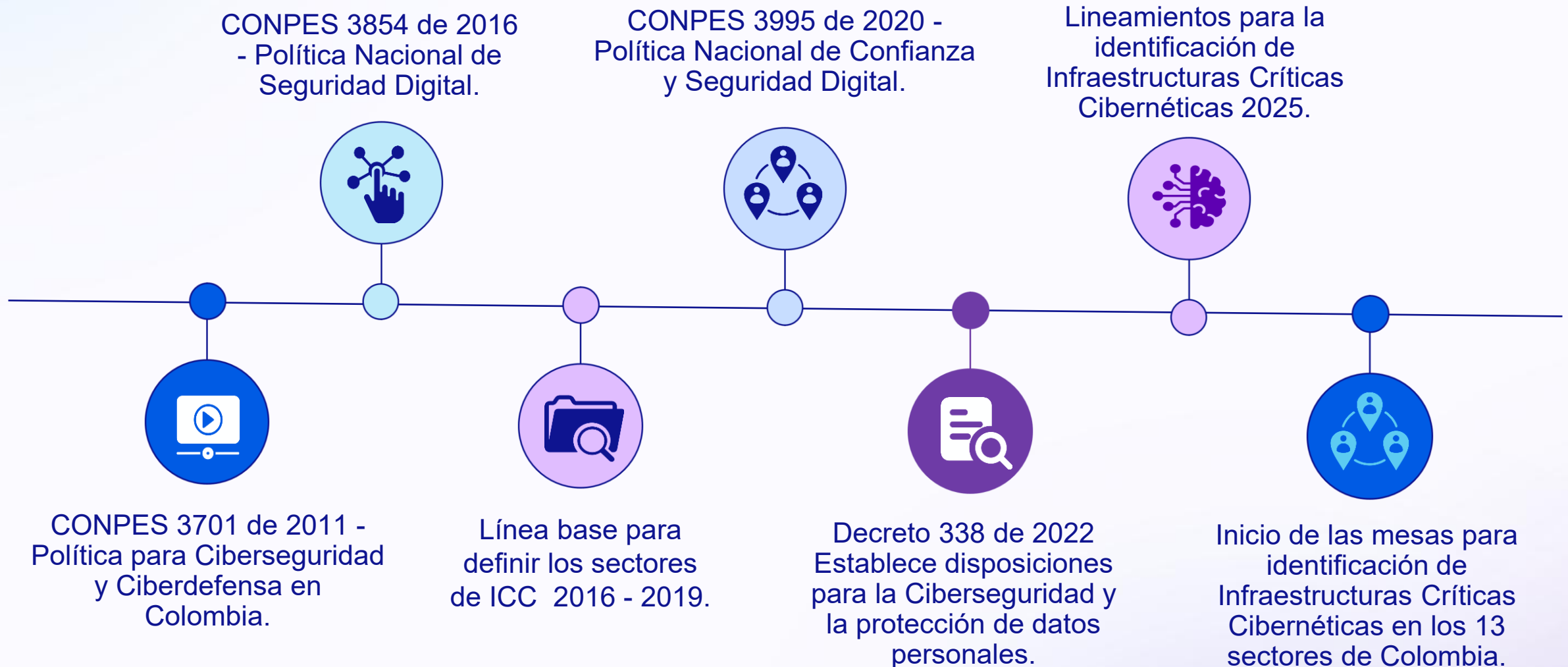
Decreto 338 de 2022 por medio del cual se establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.



Infraestructura cibernética:

Artículo 2.2.21.1.4.4. Afectación significativa. Para los efectos del presente Título, se entenderá por afectación significativa, aquella que se ocasiona a las Infraestructuras críticas cibernéticas, servicios esenciales e intereses nacionales para la seguridad digital, protección de las redes, de las infraestructuras, y los sistemas de información en el ciberespacio. Constituye la base de la actualización metodológica que aborda el documento. *"Lineamientos para la identificación de infraestructuras críticas cibernéticas"*. (GUÍA ICC – COLCERT, 2025).

Marco Legal.



Generalidades.



Infraestructura Crítica.

Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO). **(GUÍA ICC – COLCERT, 2025).**



Infraestructura Cibernética.

Cualquier sistema, ya sea físico o virtual, que sea tan vital que si se interrumpe puede tener un impacto debilitador en la seguridad, la economía, la salud pública o la seguridad, el medio ambiente. También puede definirse como los sistemas y activos que sustentan industrias o servicios urbanos y rurales subnacionales esenciales. **(GUÍA ICC – COLCERT, 2025).**



Infraestructura Crítica Cibernética.

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. **(DECRETO 338, 2022).**

Características de un Activo Crítico Cibernético.



TECNOLOGÍA DE INFORMACIÓN:
Hardware, Software, Datacenter y Redes



COMUNICACIONES:
Locales, remotas y metropolitanas.



TECNOLOGÍA DE OPERACIÓN:
Automatización y Operación Sistemas Industriales



SERVICIOS ESENCIALES.



FUNCIONES CRÍTICAS.

Servicios esenciales:

En el marco de la gestión de riesgos de la seguridad digital es aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, **(GUÍA ICC – COLCERT, 2025)**.

Ley 142 de 1994. Establece el marco jurídico para los servicios públicos domiciliarios. (acueducto, alcantarillado, aseo, electricidad y gas), y dicta disposiciones para su prestación eficiente y garantice la finalidad social del Estado.

Importancia:



¿Por qué es importante identificar las infraestructuras críticas cibernéticas?

- Es crucial para proteger los servicios esenciales y garantizar la seguridad nacional frente a posibles ciberataques.
- Esto implica reconocer qué sistemas, redes y activos digitales son vitales para el funcionamiento del país y cuya interrupción tendría graves consecuencias.
- Un ciberataque exitoso a la infraestructura crítica puede tener consecuencias devastadoras para la seguridad nacional, incluyendo interrupciones en el suministro de servicios esenciales, desestabilización social y daños económico.

Roles y Responsabilidades:



Sujetos obligados:

Serán las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones públicas o administrativas. Para los efectos del presente se les dará el nombre de autoridades.



Personas jurídicas de derecho privado:

Que presten servicios, administren, gestionen ICC o presten servicios esenciales, podrán aplicar las disposiciones del decreto, siempre que no resulten contrarias a su naturaleza y a regulaciones de su actividad o servicio. En cualquier caso, sujetarán sus actuaciones a disposiciones especiales que regulen su actividad o servicio.



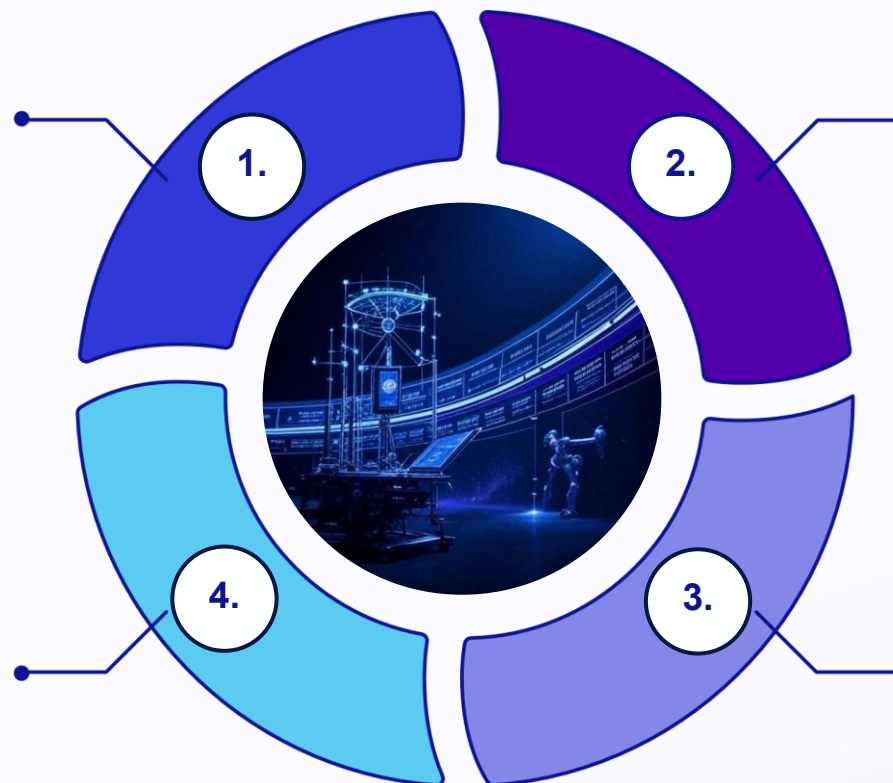
Otras ramas y organismos:

En las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113, 209 de la Constitución Política, y demás normas concordantes.



Entidades de regulación y las entidades de supervisión:

En el marco de sus competencias, evaluarán la necesidad de expedir normas para la protección de las infraestructuras críticas cibernéticas o de los servicios esenciales de su sector, y evaluarán la necesidad de proferir instrucciones a sus vigiladas para el mismo fin, según corresponda.



Amenazas a las Infraestructuras Críticas Cibernéticas.



Una falla parcial o total sobre los activos críticos de las Entidades se transforma en una vulnerabilidad crítica la cual se debe contrarrestar.

Cualquier perturbación, avería o destrucción a estos activos críticos pueden tener un grave impacto sobre los servicios o procesos esenciales de los sectores críticos nacionales (directa o indirectamente), afectando el medio ambiente, la seguridad, ciber defensa nacional y de la población, integridad de las instalaciones, el Estado, y afectando la imagen pública de las instituciones y/o produciendo cuantiosas pérdidas económicas para el país.



EVENTOS CLIMATOLÓGICOS



EVENTOS METEOROLÓGICOS



EVENTOS GEOFÍSICOS



**ACCIDENTES TECNOLÓGICOS
E INDUSTRIALES**



**INTERRUPCIONES
NO PROGRAMADAS**



**INCIDENTES CRIMINALES
Y ATAQUES TERRORISTAS**



INCIDENTES CIBERNÉTICOS

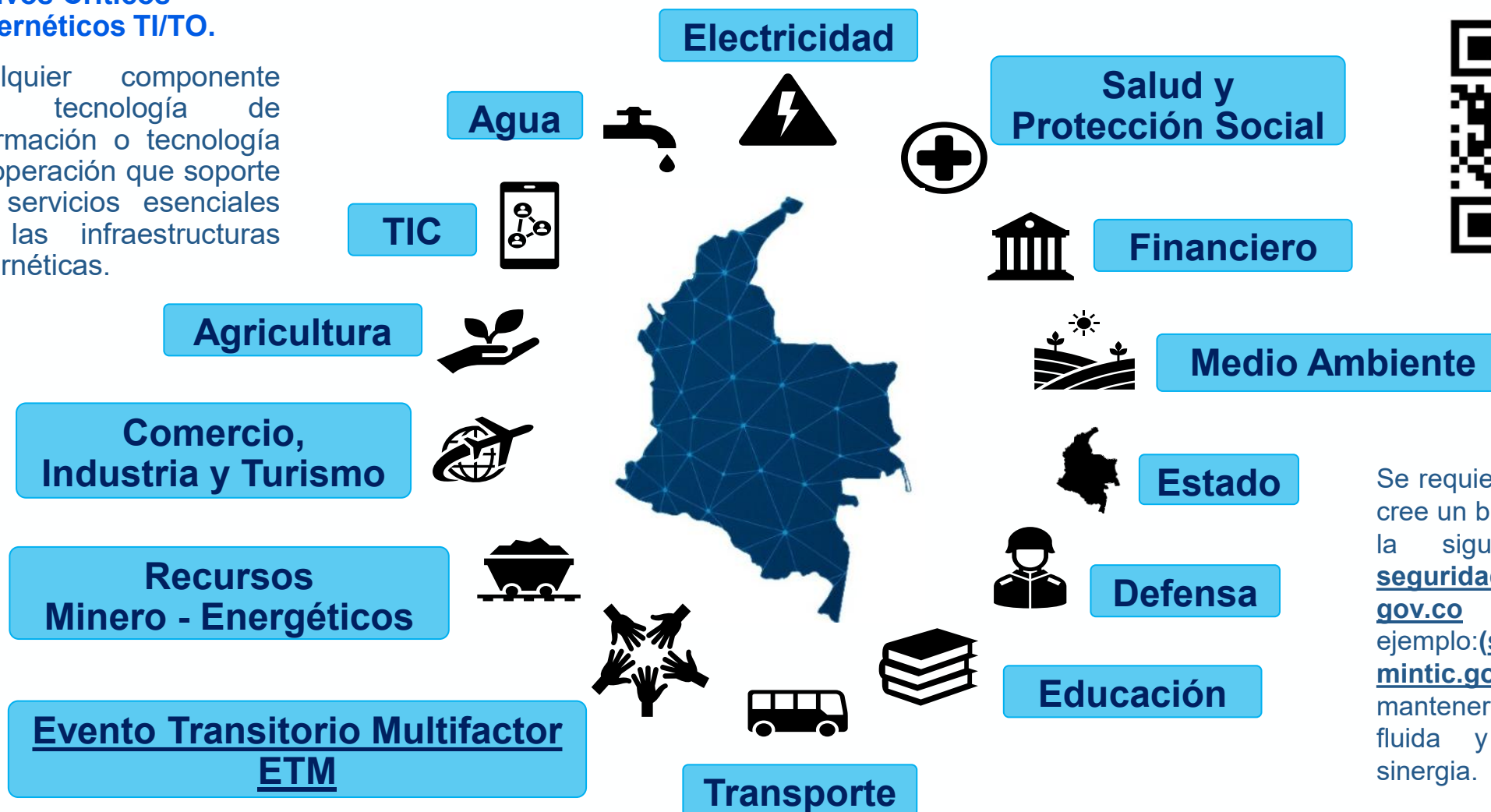
**OPERACIONES DE INFLUENCIA
EXTRANJERA
INVERSIÓN NO CONFIABLE**

Sectores Críticos Identificados:

14 sectores de infraestructura crítica para Colombia.

Activos Críticos Cibernéticos TI/TO.

Cualquier componente con tecnología de información o tecnología de operación que soporte los servicios esenciales en las infraestructuras cibernéticas.



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.

Actividades Primarias.

Designación Autoridad líder del sector:



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.

Trabajo de campo:



Aplicación de la metodología (Instrumento) y aplicación de las variables para identificación de ICC.



Designación líder de equipo:

La Autoridad también deberá elegir un "Líder del Equipo de Planificación". Una vez hecho esto, deberán revisar cualquier documentación o gobernanza actual existente.



Definir dependencias (Matriz) - RACI:

En Colombia se propone esta interrelación la cual varió acorde al levantamiento y actualización en el inventario de la Infraestructura Crítica cibernética. Este paso identifica 13 sectores y explica la interrelación que se pretende lograr a partir del levantamiento de la ICC. (Ver Matriz)

Matriz de Interdependencias por sector.

		1	2	3	4	5	6	7	8	9	10	11	12	13
														
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		●					●						●	●

Definición de la variable y metodología.

Paso 1:



Identifique los activos críticos de información de su entidad según los lineamientos establecidos en el Modelo de Privacidad y Seguridad de la Información (MSPI) publicado por el Ministerio de Tecnologías de la información y las comunicaciones.

Mantenimiento funciones sociales, económicas Nacional o información estratégica para el Estado -

Actividad o servicios Dependencia infraestructura TI/TO (**Decreto 338 - Sección 4 .)**

Paso 2:



Realice el análisis y evaluación de riesgos a los activos identificados centrándose en los activos críticos o en los procesos misionales según los lineamientos de gestión de riesgos asociada al MSPI.

Paso 3:



Con base en el paso 1 y 2 diligencie la matriz en formato Excel denominado **Anexo 1**, con los activos o servicios identificados como críticos.



Definición de la variable y metodología.

Continuación Paso 3:



Una vez, diligenciado el Anexo 1, anonimice la información asociada en los ítems color naranja que corresponde a las variables para la identificación de las ICC. 46

Generar el pasó a pasó del diligenciamiento del Excel con cada una de las observaciones generadas en los comentarios para el entendimiento y diligenciamiento de las entidades u organizaciones.

Paso 4:



Deberá diligenciar el siguiente formulario <https://forms.office.com/r/bvYF1QCBUF>, denominado **Anexo 2**, con el fin de evaluar el estado de madurez y la infraestructura crítica cibernética de cada organización.

Paso 5:



Enviar al correo icc@colcert.gov.co los anexos 1 y 2 diligenciados, referenciando nombre de la entidad, responsable, correo electrónico institucional y número de teléfono del responsable.



Definición de la variable y metodología.



1. Impacto operacional.

Mide el alcance e impacto en el funcionamiento, considerando **factores como salud pública y el área geográfica afectada** en caso de interrupción de un servicio de infraestructura crítica. Incluye aspectos como: **cantidad de usuarios y distribución geográfica de la infraestructura**. Su evaluación es clave para identificar zonas vulnerables y desarrollar planes de contingencia específicos.

2. Contexto y/o población afectada.

Identifica el contexto y la relevancia del sistema, **considerando la cantidad de personas impactadas por la interrupción** de un servicio de infraestructura crítica, así como la densidad poblacional en la zona de influencia. Con un enfoque basado en Derechos Humanos, se evalúa el impacto en la afectación de la población, destacando su importancia para determinar la prioridad en la recuperación del servicio.

3. Impacto a las funciones críticas nacionales.

Evalúa el impacto sobre **cuántas funciones críticas nacionales se ven alteradas** 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.

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.

Esta variable evalúa los incidentes que podrían **afectar los servicios del Estado, considerando aspectos de seguridad nacional, derechos humanos y la afectación correlacionada con otros sectores esenciales o interdependientes**. Se analiza el impacto del servicio y su relación de interdependencia con otros sectores para determinar su relevancia a nivel nacional.

Definición de las variables y metodología.



1. Impacto operacional.

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

Moderado (2) = Nivel moderado: 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.

2. Contexto y/o población afectada.

Bajo (1) = 99.999 o menos personas.

Moderado (2) = de 100.000 a 249.999 personas.

Alto (3) = de 250.000 a 499.999 personas.

Extremo (4) = Impacto potencial a 500.000 o más personas.

3. Impacto a las funciones críticas nacionales.

Bajo (1) = Una o ninguna función crítica.

Moderado (2) = Dos funciones críticas con impacto en su organización y otros sectores.

Alto (3) = Tres funciones críticas nacionales, y que afecte a otras organizaciones.

Extremo (4) = Cuatro o más funciones críticas nacionales, se refleja en la capacidad operativa de la organización, impacto conocido o previsto en otras organizaciones.

4. Afectación Económica Nacional.

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

Moderado (2) = Impacto entre el 0,1 al 0,5%

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

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

5. Impacto Nacional al servicio.

Bajo (1) = Improbable que afecte a otras organizaciones.

Moderado (2) = Posibilidad mínima de impacto para otras organizaciones.

Alto (3) = Es probable que afecte a otras organizaciones.

Extremo (4) = Impacto conocido o previsto en otras organizaciones.

Anexo 1.



Sub sector	Gasto						
Servicio esencial prestado	Categoría de Funciones Críticas Nacionales	Funciones Críticas Nacionales	Activos Cibernéticos (infraestructura ICC)	Pilares de Seguridad de la Información	Amenaza (tipo de incidente)	Tiempo de indisponibilidad	Impacto en las Funciones Críticas Nacionales
							10
7. Telecomunicaciones: Telefonía pública básica conmutada y móvil rural: Servicios de comunicación. (Ley 142 de 1994)	ConexiónComunicación	3. Prestación de servicios de comunicación e información de contenidos basados en Internet	XXX	Confidencialidad	1. Obtención de información: Métodos para acceder a datos sensibles.	1	1

- 1. La ICC entre 2,95 a 4. (Categoría Crítico) - Extremo
- 2. La ICC entre 1,95 y 2,94. (Categoría Esencial) - Alto
- 3. La ICC entre 0,95 y 1,94. (Categoría importante) - Moderado
- 4. Activo < 0,95 que se contempla, pero no cumple un impacto a nivel nacional. – (Categoría Secundario) - Bajo

Anexo 1 - Matriz RACI.

SECTOR:									
ENTIDAD:									
INFRAESTRUCTURA / ACTIVIDAD	Alimentación y agricultura	Agua	Comercio, industria, turismo	Defensa	Educación	Electricidad	Financiero	Gobierno/Estado	R

Responsable (R): Quien ejecuta la tarea (solo un único responsable por actividad / Activo para evitar confusión).

Consultado (C): Quien aporta conocimiento o experiencia (puede haber varios).

Informado (I): Quien debe ser actualizado sobre el progreso, pero no interviene directamente (puede haber varios).

Sin Interacción (S/I) Que no tiene interacción con la actividad, (puede haber varios).

Taller:

Fuentes para identificar actividad esencial / Servicios prestados?



A continuación podrá consultarse el Manual de Estructura del Estado elaborado por Función Pública. Esta herramienta virtual presenta a la ciudadanía y a sus grupos de valor la organización y estructura del Estado colombiano en sus diferentes componentes y las normas que lo sustentan.

El Manual está organizado en bloques temáticos correspondientes a las Ramas del Poder Público: Legislativa, Ejecutiva y Judicial; los órganos autónomos e independientes; el Sistema Integral de Verdad, Justicia, Reparación y No Repetición; la organización electoral y los organismos de control, los cuales contribuyen al cumplimiento de las funciones del Estado. En cada una de las entidades que integran el Estado se encuentran los organigramas, las normas de estructura orgánica, el objetivo y sus funciones.

Esta versión digital facilita el acceso democrático, oportuno, transparente y sencillo a la información del Estado colombiano.



Conozca la Estructura del Estado, navegando el siguiente organigrama:



*Ramas del Poder Público: Es el conjunto de instituciones públicas que, por mandato de la Constitución Política, ejercen de manera permanente las funciones del Estado.

Estructura del Estado

Rama Ejecutiva

- Orden Nacional
- Orden Departamental
- Orden Municipal

Rama Legislativa

Rama Judicial

Organización Electoral

Órganos Autónomos e Independientes

Organismos de Control

Sistema Integral de Verdad, Justicia, Reparación y No Repetición



Rama Ejecutiva del Orden Nacional

A la Rama Ejecutiva le corresponde ejecutar, en forma coordinada, todas las actividades administrativas que están al servicio de los intereses generales de la comunidad para el cumplimiento de los fines esenciales del Estado. Está representada por el Presidente de la República, quien simboliza la unidad nacional, es el Jefe de Estado, Jefe de Gobierno y suprema autoridad administrativa.

El Gobierno Nacional está formado por el Presidente de la República, los ministros del despacho y los directores de departamentos administrativos. El Presidente y el Ministro o Director de Departamento correspondientes, en cada negocio particular, constituyen el Gobierno.

La Rama Ejecutiva tiene 3 órdenes: nacional, departamental y municipal.

La organización territorial se asimila al concepto de ordenamiento territorial, el cual hace relación al conjunto de normas que establecen y regulan, por disposición de la Constitución, la forma como se distribuye espacialmente el poder público entre los diversos niveles político-administrativos de autoridad establecidos por la Carta Política (nacional, departamental, distrital y municipal).



Navegue el siguiente organigrama:

Taller:

Fuentes para identificar actividad esencial / Servicios prestados?



Nombre del sistema/aplicativo relevante	Breve descripción del sistema/aplicativo	¿La entidad tiene clasificado el sistema/aplicación como un activo crítico?		¿Tiene identificada la infraestructura que soporta el sistema/Aplicativo?		¿El sistema/aplicativo procesa/almacena datos personales / Sensibles?		¿El sistema/aplicativo procesa información pública reservada?		¿El sistema/aplicativo Soporta los procesos misionales de la entidad?		¿Se causan pérdidas económicas significativas si el sistema/aplicativo deja de funcionar, más allá del RTO?		¿Del sistema/aplicativo dependen uno o más sistemas internos?		¿Del sistema/aplicativo dependen uno o más sistemas externos?
		SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	
Saludtools	mas el control, de las solicitudes de preparacion por parte de hospitales y clientes de la radiofarmacia. Tipo Cloud, alojando en hosting AWS geolocalizado en holanda	X		X		X		X		X		X		X		

Taller:

¿Sistemas o activos críticos?



1.

SIIF NACIÓN

- ¿Cuántos activos están detrás de SIIF?
- ¿Cuántos usuarios tiene?
- ¿Con qué entidades interactúa?
- ¿Qué servicios esenciales del Estado colapsan?
- ¿Qué servicios geográficos afectan?



2.

MUISCA - DIAN

- ¿Qué sector es líder frente a este activo?
- ¿Afecta a las regiones?
- ¿Cuál es el RTO nacional para este activo?
- ¿Cuál es el RPO nacional para este activo?
- ¿Los dispositivos primarios son más críticos que sus respaldos?



3.

SECOP II

- ¿Puede funcionar el Estado sin SECOP?
- ¿Cuál es el costo económico de una falla, más allá del RTO?
- ¿Con qué entidades interactúa?
- ¿Qué servicios esenciales del Estado Colapsan?
- ¿Qué servicios geográficos afectan?

Taller:

¿Sistemas o activos críticos?



1. Impacto operacional.



- Plataforma integral para la gestión de ingresos, servicios y control fiscal y aduanero.
- Gestión de facturación electrónica, Consulta y pago de impuestos.
- Trámites aduaneros (importación y exportación).
- Consulta y actualización del RUT.

2. Contexto y/o población afectada.



EL TIEMPO

SUSCRÍBETE

INICIAR SESIÓN

ECONOMÍA | SECTORES | FINANZAS PERSONALES | EMPRESAS | SECTOR FINANCIERO

NOTICIA

Alerta entre contribuyentes por las fallas presentadas en el sistema de la Dian

Entidad declaró indisponibilidad de los servicios informáticos por incidentes técnicos.



3. Impacto a las funciones críticas nacionales.



MINISTERIO DE HACIENDA Y
CRÉDITO PÚBLICO

4. Afectación Económica Nacional.



CARACOL
RADIO

Escúchalo con el programa

Economía

Trámites de importaciones y exportaciones se ven afectados por fallas externas a la Dian: Qué hacer

La Dirección de Impuestos y Aduanas Nacionales informó que fallas son externas.



Últimas Noticias

Fue condenado un hombre a más de 45 años de cárcel por feminicidio en El Bagre

5. Impacto Nacional al servicio.

Estructura del Estado



Fortaleciendo la Seguridad Digital:



1. **Estrategias Clave Implementar Modelos de Seguridad:** Adoptar MSPI/SGSI basados en estándares nacionales e internacionales.
2. **Planes Estratégicos:** Diseñar políticas y controles de seguridad digital.
3. **Recuperación ante Desastres:** Establecer planes DRP para continuidad tecnológica.
4. **Actualización de Sistemas:** Mantener al día software crítico, navegadores y antivirus.
5. **Protección de Red:** Usar firewalls e IPS para filtrar tráfico y bloquear amenazas.
6. **Inspección TLS/SSL:** Detectar amenazas en tráfico cifrado.
7. **Sandboxing:** Analizar archivos sospechosos en entornos virtuales seguros.

Fortaleciendo la Seguridad Digital:



8. Autenticación Multifactor (MFA): Reforzar el control de acceso.

9. Capacitación de Usuarios: Formar al personal contra nuevas ciberamenazas.

10. Cifrado de Datos: Proteger datos sensibles y copias de seguridad.

11. Monitoreo Continuo: Detectar y responder rápidamente a amenazas.

12. Gestión de Activos Críticos: Identificar y analizar riesgos en la infraestructura.

13. Respuesta a Incidentes: Desarrollar planes efectivos de gestión de crisis.

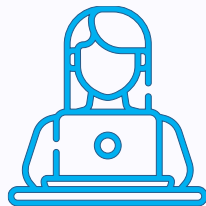
14. Copias de Seguridad: Automatizar backups periódicos para recuperación.

Conéctate con el ColCERT:



Reporte de incidentes.

csirtgob@mintic.gov.co
Entidades de Gobierno



contacto@colcert.gov.co
Privados

icc@colcert.gov.co
Temas de ICC

Sitio web.



Alertas y boletines



@colCERT

Registro y Actualización de Datos
de Contacto para CISOs y Oficiales
de Seguridad



Línea directa:
[+57 601 344 2222](tel:+576013442222)





Ministerio de Tecnologías de la Información y las Comunicaciones

2025

 [ministerio_tic](#)

 [@ministerio_tic](#)

 [@ministerio_tic](#)

 [@Ministerio_TIC](#)

 [MinisterioTIC.Colombia](#)

 [@ministeriotic](#)

 [@MinisterioTIC_Colombia](#)