ARTÍCULO DOI 10. 52781/cmm.a157

El papel del Sistema de Ingeniería del Ejército Brasileño en la seguridad de la Infraestructura Crítica de Transporte

The role of the Brazilian Army Engineering System in the Critical Transportation Infrastructure Security

Resumen: Las infraestructuras críticas son activos expuestos a riesgos asociados a amenazas humanas o desastres naturales, en los que se basa la sociedad para mantener la economía, la salud y la seguridad pública. Muchos países han elaborado planes específicos para garantizar la seguridad de infraestructuras críticas mediante la cooperación entre autoridades, agencias y el sector privado. Consciente de las capacidades del Ejército Brasileño para actuar en la construcción de infraestructuras de transporte, el autor buscó en este artículo relacionar las actividades realizadas por el Sistema de Ingeniería del Ejército Brasileño con la capacidad de garantizar la seguridad de la Infraestructura Crítica de Transporte. Finalmente, se constató que el Sistema de Ingeniería ha contribuido a la seguridad al actuar en la gestión y mitigación de los riesgos mediante la ejecución de obras y servicios de ingeniería, proporcionando una mayor resiliencia a las infraestructuras físicas terrestres.

Palabras clave: Infraestructuras críticas. Ingeniería del Ejército Brasileño. Gestión de riesgos. Transportes. Inundaciones.

Abstract: Critical infrastructure are assets subject to risks associated with human threats or natural disasters, on which society relies to maintain economy, health and public safety. Several countries have developed specific plans to ensure the security of critical infrastructure through cooperation between authorities, agencies and the private sector. Aware of the capabilities of the Brazilian Army to act in the construction of transport infrastructure, the author sought in this article to relate the activities performed by the Brazilian Army Engineering System with the ability to guarantee the security of the Critical Transport Infrastructure. Finally, it was noted that the Engineering System has collaborated with security by acting in risk management and mitigation by civil construction and engineering services, providing greater resilience to transportation infrastructure.

Keywords: Critical infrastructure. Brazilian Army Engineering. Risk management. Transportation. Floods.

Halan Bastos Oliveira
Universidade Federal do Rio de Janeiro.
Programa de Engenharia Urbana.
Exército Brasileiro. Comissão Regional de Obras 7.
Recife, PE, Brasil.
halan_bastos@hotmail.com

Recibido: 27 jun. 2023
Aprobado: 17 feb. 2025

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUCCIÓN

La *Cybersecurity and Infrastructure Security Agency* (Cisa) define las Infraestructuras Críticas (IC) como cualquier activo, sistema, instalación, red u otros elementos de los que se basa la sociedad para mantener la economía, la salud y la seguridad pública. Fenómenos climatológicos y meteorológicos extremos, ataques a carreteras y ferrocarriles, además de pandemias o ataques terroristas son algunos de los riesgos a los que están expuestas las IC de una nación (EE.UU., 2019).

El *Centre for the Protection of National Infrastructure* (CPNI) (Reino Unido, 2023) define las IC como instalaciones, sistemas, lugares, informaciones, personas, redes y procesos necesarios para el funcionamiento de un país y de los cuales depende la vida cotidiana. También incluye algunas funciones, lugares y organizaciones que no son críticas para el mantenimiento de servicios esenciales, pero que requieren protección debido al peligro potencial para el público, como instalaciones nucleares y químicas civiles, por ejemplo. Los daños o la destrucción de IC causados por catástrofes naturales, terrorismo o actividades criminales pueden tener consecuencias negativas para la seguridad del país y el bienestar de sus ciudadanos.

Aunque no hay una definición formal de "Infraestructura Crítica", diversos organismos gubernamentales desarrollan sus propias legislaciones para determinar qué partes de sus infraestructuras son cruciales. Sin embargo, estas definiciones suelen ser genéricas porque proporcionan una perspectiva estratégica que posteriormente se debe analizar sector por sector.

Algunos países ya cuentan con un plan de defensa de IC, incluso con organismos dedicados a esta función, como por ejemplo la Cisa en Estados Unidos, cuya misión es defender los activos cibernéticos y la infraestructura del país y colaborar con la construcción de estructuras más seguras y resilientes (Estados Unidos de América, 2023). En Reino Unido, además de ser frecuentemente reclasificados por el CPNI, los sectores de infraestructura se subdividen en "subsectores", como los de policía, ambulancia, bomberos y guardia costera, que pertenecen al servicio de emergencia. Cada uno de ellos cuenta con, al menos, un departamento gubernamental responsable de garantizar la seguridad de sus activos (Reino Unido, 2023).

La Infraestructura Crítica de Transporte (ICT), además de la propia estructura física de carreteras, ferrocarriles y aeropuertos, también abarca el transporte de cargas y de pasajeros. Desastres naturales, actos de terrorismo, sabotaje o guerra, junto con el desarrollo humano desordenado en áreas urbanas, constituyen los principales riesgos a los que están expuestas estas estructuras.

En Brasil, la Cámara de Diputados aprobó las actualizaciones de la Política Nacional de Defensa (PND) y de la Estrategia Nacional de Defensa (END) en diciembre de 2024 y, tras su aprobación, pasaron a promulgación (Cámara..., 2024). Aunque uno de los objetivos de los documentos es concienciar a toda la sociedad sobre la importancia de la defensa del País (Brasil, 2023, p. 71), Rocha (2019) menciona la negligencia de las autoridades en prevención y seguridad frente a amenazas o ataques debido a la cultura pacífica y a la ausencia de conflictos recientes con otras naciones. El tema de la defensa de IC, por ejemplo, solo se introdujo en un documento oficial en 2008 y de una forma muy discreta, sin la definición del término o la clasificación de los activos críticos de infraestructura del país (Brasil, 2008).

Solo se aprobó el Plan Nacional de Seguridad de Infraestructuras Críticas (Plansic) en septiembre de 2022 (Brasil, 2022), con el objetivo de crear la estructura operativa que sustentará el

seguimiento y monitoreo permanente de la seguridad de las IC del país. Sin listar nominalmente las estructuras a observar, el Plan define de forma genérica y con plazos amplios los responsables de desarrollar acciones específicas para cada sector de IC.

Sin embargo, el Ejército Brasileño, en su atribución subsidiaria de cooperar con el desarrollo nacional y la defensa civil (Brasil, 1999, art. 16), actúa en la construcción, mantenimiento y protección: de la infraestructura de fortificaciones desde el período del Brasil Colonial; de la red ferroviaria y líneas telegráficas desde el Brasil Imperial; y, ya en el período republicano, de carreteras que conectan las diversas regiones del país (Figueiredo y colaboradores, 2014), incluso mediante alianzas con empresas privadas para ejecutar obras y servicios de ingeniería (Brasil, 1999, art. 17A).

En este sentido, este estudio trata del papel del Sistema de Ingeniería del Ejército Brasileño (SEEx) en la ejecución de las acciones de seguridad de la Infraestructura Crítica de Transporte de Brasil desde la perspectiva de las misiones constitucionales y atribuciones subsidiarias de la institución, con un enfoque cualitativo mediante el análisis de los dispositivos legales y de investigación bibliográfica relacionada con el tema. Además, como la investigación bibliográfica ha indicado un mayor nivel de madurez sobre el tema en la literatura extrajera, este artículo también buscar colaborar con la literatura nacional sobre el tema de la seguridad de IC.

2 METODOLOGÍA

2.1 La ICT en el escenario internacional

Desde mediados de la década de 2000, los gobiernos han proyectado e implementado políticas públicas para apoyar la protección de la IC. La mayoría de los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2019) definió sectores de IC, elaboró un inventario de activos e implementó regulaciones, programas nacionales y mecanismos de incentivo para fortalecer la resiliencia de estas estructuras frente a peligros o amenazas.

En Estados Unidos, debido al desarrollo económico y al historial de guerras y amenazas terroristas que suele enfrentar, la concienciación sobre el tema de la IC empezó mucho antes que en Brasil. El gobierno norteamericano, tras los ataques terroristas del 11 de septiembre de 2001, publicó una serie de directrices de seguridad interna con el objetivo de elaborar un plan nacional integral para garantizar la seguridad de las IC a través de la cooperación de las autoridades y de las agencias federales, regionales y locales, así como del sector privado y de otras entidades (Brasil, 2020, art. 4).

El Consejo de la Unión Europea, al definir ampliamente las IC como activos y sistemas esenciales para mantener las funciones vitales de la sociedad, se concentró específicamente en los sectores de energía y transporte, cuya perturbación o destrucción afectaría a uno o más Estados miembros, y estos impactos deben evaluarse con base en criterios integrales, incluidos los efectos que resultaron de dependencias intersectoriales en relación con otros tipos de infraestructuras.

Además, en 2007, el mismo Consejo aprobó una serie de conclusiones sobre el Programa Europeo de Protección de Infraestructuras Críticas (Pepic), y reafirmó que, en última instancia, cada Estado miembro es responsable de garantizar la protección de las IC en sus respectivos territorios nacionales. Esta dinámica condujo a la publicación, en 2008, de la Directiva del Consejo

Europeo sobre identificación y designación de las IC Europeas, estableciendo un procedimiento para su identificación y designación, así como un enfoque común para evaluar la necesidad de mejorar su protección (Natário; Nunes, 2014).

El estudio de Natário y Nunes (2014), realizado a partir de la recopilación de informaciones del *International CIIP Handbook 2008/2009* (*apud* Brunner; Suter, 2008), constató que, entre los 25 países investigados (Tabla 1), Estados Unidos (EE.UU.), seguido de Noruega, fueron los países con más infraestructura clasificada como crítica durante el período de obtención de los datos, entre 2008 y 2009. Solamente Rusia no clasificó el sector de Transportes/Logística como crítico.

Tabla 1. Sectores considerados críticos en diversos países, con las siglas según la norma ISO 3166 (ISO, 2020)

PAÍSES / SECTORES	AUS	AUT	BRA	CAN	EST	FRA	FIN	DEU	HUN	IND	ITA	JPN	KOR	MAL	NLD	NOR	NZL	POL	RUS	SWE	SGP	ESP	CHE	GBR	USA	Total de países
Bancos y Finanzas	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	25
Gobierno Central		•		•	•	•		•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•	20
Industrias Química y Nuclear				•						•				•	•			•				•	•		•	8
Servicios de Emergencia	•		•	•	•	•			•	•	•		•	•		•	•	•	•				•	•	•	17
Electricidad/Energía	•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•			•	•	•	•	•	21
Agricultura/ Alimentación	•			•	•	•	•	•	•		•	•			•	•					•	•	•	•	•	16
Servicios de Salud	•		•	•	•	•	•		•		•			•	•	•					•	•	•	•	•	16
Comunicación/Medios de Comunicación	•	•				•	•		•		•		•		•	•			•	•	•		•		•	14
Defensa						•			•	•			•	•		•			•					•	•	9
Monumentos Nacionales	•																								•	2
Aguas residuales/ Residuos	•										•			•	•	•		•					•	•	•	9
Telecomunicaciones	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•		•	•	23
Transportes/Logística	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	24
Distribución de Agua	•		•		•	•	•	•	•		•	•		•	•	•				•	•	•	•	•	•	18
Total de sectores	11	6	6	9	9	11	8	7	11	7	11	7	8	9	11	12	6	8	6	6	8	9	11	11	14	

Fuente: Adaptado de Natário y Nunes (2014).

Con la evidente interdependencia de estos activos de infraestructura, en 2019 la OCDE realizó otro estudio con sus países miembros, considerando 16 sectores (y 1 adicional genérico) potencialmente críticos. El informe concluyó que, salvo Estonia, todos los demás 31 países de la OCDE clasifican la infraestructura de transportes como crítica, ocupando este sector el segundo lugar en términos de criticidad, siendo el primero el sector eléctrico (Tabla 2).

Liu y Song (2020) señalan que carreteras, ferrocarriles y aeropuertos son infraestructuras esenciales para el funcionamiento de la cadena logística de casi todos los servicios vitales para la sociedad, y que fallas o ataques contra algunos de ellos pueden desencadenar una serie de consecuencias de bajo impacto, como congestionamientos, o catastróficas, como ataques terroristas. En entornos urbanos, donde normalmente existe una mayor densidad demográfica, incluso

fallas simples en estas estructuras, como la obstrucción de sistemas colectores de aguas pluviales o baja adherencia del pavimento, provocan pérdidas humanas. Fenómenos naturales como lluvias intensas, terremotos o huracanes, que además no pueden ser controlados por el ser humano, son una de las principales amenazas para la ICT de una ciudad.

Tabla 2. Sectores considerados críticos en los países de la OCDE, con las siglas según la norma ISO 3166 (ISO, 2020)

PAÍSES / SECTORES	AUS	AUT	BEL	CAN	CHE	CHL	CZE	DEU	ESP	EST	FIN	FRA	GBR	GRC	IRL	ISL	ISR	ITA	KOR	LAT	LUX	MEX	NLD	NOR	NZL	POL	PRT	SVK	SVN	SWE	TUR	USA	Total de países
Energía	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	32
Industria Nuclear				•			•		•			•	•				•		•					•	•							•	10
TI y Comunicación	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	31
Transportes/ Logística	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	31
Distribución de agua	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•	•	•		•				•	22
Represas e inundaciones	•					•	•					•			•	•		•	•	•		•	•	•				•		•	•	•	15
Suministro y distribución de alimentos	•	•		•	•		•	•	•		•	•	•				•				•			•		•				•	•	•	17
Servicios de salud	•	•	•	•	•	•	•	•	•	•	•	•	•				•		•	•	•			•		•		•		•	•	•	23
Bancos y Finanzas	•	•	•	•	•		•	•	•	•	•	•	•				•		•	•	•		•	•		•		•		•	•	•	23
Gobierno		•		•	•		•	•	•			•	•				•		•	•	•			•		•				•		•	16
Seguridad Pública	•	•		•	•		•	•	•				•				•			•	•		•	•						•		•	15
Aplicación de la ley		•				•		•				•	•				•			•	•		•	•									10
Industria Química	•	•			•				•		•	•	•				•			•	•		•	•		•		•				•	15
Sector espacial			•						•			•	•																				4
Industria de Defensa	•										•	•	•				•			•												•	7
Industria de fabricación				•							•	•					•							•							•	•	7
Otros		•	•					•	•	•	•	•	•				•		•	•	•		•	•	•	•				•	•	•	19
Total de sectores	11	12	8	11	10	6	11	11	13	6	11	16	15	3	4	4	15	4	10	13	12	4	11	15	5	10	2	7	4	9	9	15	

Fuente: OCDE (2019).

2.2 Historia de la Seguridad de Infraestructuras Críticas en Brasil

En Brasil, solamente en 2006, tras ataques de la facción criminal *Primeiro Comando da Capital* (PCC por sus siglas en portugués, que se puede traducir como Primer Comando de la Capital) en el estado de São Paulo, la Oficina de Seguridad Institucional de la Presidencia de la República inició la identificación y el análisis de riesgos de las IC del País (Rocha, 2019), empezando con las áreas de comunicación, energía, transporte y agua, en asociación con organismos públicos y entidades privadas. Así, se mencionó por primera vez el término "Infraestructuras

Críticas" en un documento oficial en 2008, en la primera versión de la END, como elemento prioritario de la acción estratégica "Seguridad Nacional", que tenía el objetivo de que todo el Estado colaborara para prevenir riesgos y aumentar la seguridad en el país (Brasil, 2008).

El 22 de noviembre de 2018, mediante el Decreto Presidencial nº 9.573, se aprobó la Política Nacional de Seguridad de Infraestructuras Críticas (PNSIC) para definir las directrices relativas al esfuerzo conjunto que los organismos públicos y las entidades privadas deben desarrollar con respecto a la seguridad de IC, correspondiendo a la Cámara de Relaciones Exteriores y Defensa Nacional del Consejo de Gobierno analizar, discutir y proponer la Estrategia Nacional de Seguridad de Infraestructuras Críticas (ENSIC) y el Plansic.

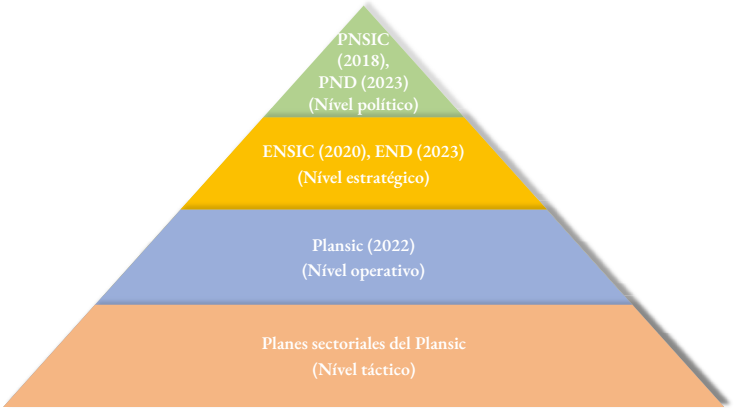
Además, la PNSIC enmarcó la seguridad de estas infraestructuras como una actividad prioritaria del Estado, elevada a nivel institucional. Para lograr los objetivos, serían necesarios tres instrumentos: la Estrategia Nacional de Seguridad de Infraestructuras Críticas; el Plan Nacional de Seguridad de Infraestructuras Críticas; y el Sistema Integrado de Datos de Seguridad de Infraestructuras Críticas (Brasil, 2018a).

Dos años tras la aprobación de la PNSIC, ya el 9 de diciembre de 2020, la Presidencia de la República, mediante el Decreto nº 10.569, aprobó la ENSIC, para identificar los riesgos a los que están expuestas las IC de Brasil y para definir las principales acciones a adoptarse para asegurar la integridad de la prestación de servicios indispensables al Estado y a la sociedad brasileña (Brasil, 2020, art. 5).

El 15 de septiembre de 2022, mediante el Decreto nº 11.200, se aprobó el Plan Nacional de Seguridad de Infraestructuras Críticas (Plansic) con el objetivo de identificar las IC del país; analizar los riesgos y la interdependencia de las IC; evaluar las vulnerabilidades y proponer medidas para eliminar o reducir las debilidades de las IC, aumentando su resistencia ante amenazas, entre otros objetivos. Además, el Plansic prevé la creación de Planes Sectoriales complementarios para tratar de las acciones de seguridad en cada sector, dependiendo esencialmente de la actuación integrada de las tres esferas de gobierno para su implementación (Brasil, 2022).

En la primera etapa del Plan, se definieron las acciones estratégicas con el objetivo de construir una estructura de gobernanza, iniciativas de capacitación y concienciación de los actores involucrados y establecer las herramientas de almacenamiento, gestión e integración de los datos e informaciones (Brasil, 2022).

Figura 1. Diferentes niveles de legislación sobre Seguridad de Infraestructuras Críticas



Fuente: elaborado por el autor.

Comparando las legislaciones presentadas con los diferentes niveles de planificación y conducción de las operaciones militares del Sistema de Planificación Conjunta de Empleo de las Fuerzas Armadas (SisPECFA) (Brasil, 2017b, p. 2-10), se puede afirmar que el Plansic es el primero a tratar de la seguridad de las IC a un nivel operativo, asignando responsabilidades específicas, estableciendo plazos, aunque amplios, y definiendo metas, aunque genéricas, a partir de cada acción estratégica (Figura 1). Así, el Plan debe desempeñar un papel crucial en el vínculo entre los objetivos estratégicos y la implementación táctica, una vez creados los respectivos Planes Sectoriales.

El Plansic, como planificación a nivel operativo, aún debe ajustarse según las condiciones establecidas por los actores políticos, como el tiempo y los recursos disponibles, y también por el propósito requerido por las acciones tácticas, pero, a la vez, debe garantizar el soporte logístico necesario y proveer los recursos necesarios para el cumplimiento de los objetivos estratégicos.

Los Planes Sectoriales serán documentos complementarios al Plan que proporcionarán directrices sobre los niveles deseables de protección, las actividades de seguridad a realizar y la priorización en la asignación de recursos, teniendo en cuenta las particularidades y tratando específicamente de las acciones de seguridad de cada sector. Tanto la implementación del Plansic como la de los Planes Sectoriales tendrán el apoyo del Ministerio de Defensa, según lo establecido por la END (Brasil, 2022, p. 5).

2.3 Identificación de la ICT Nacional

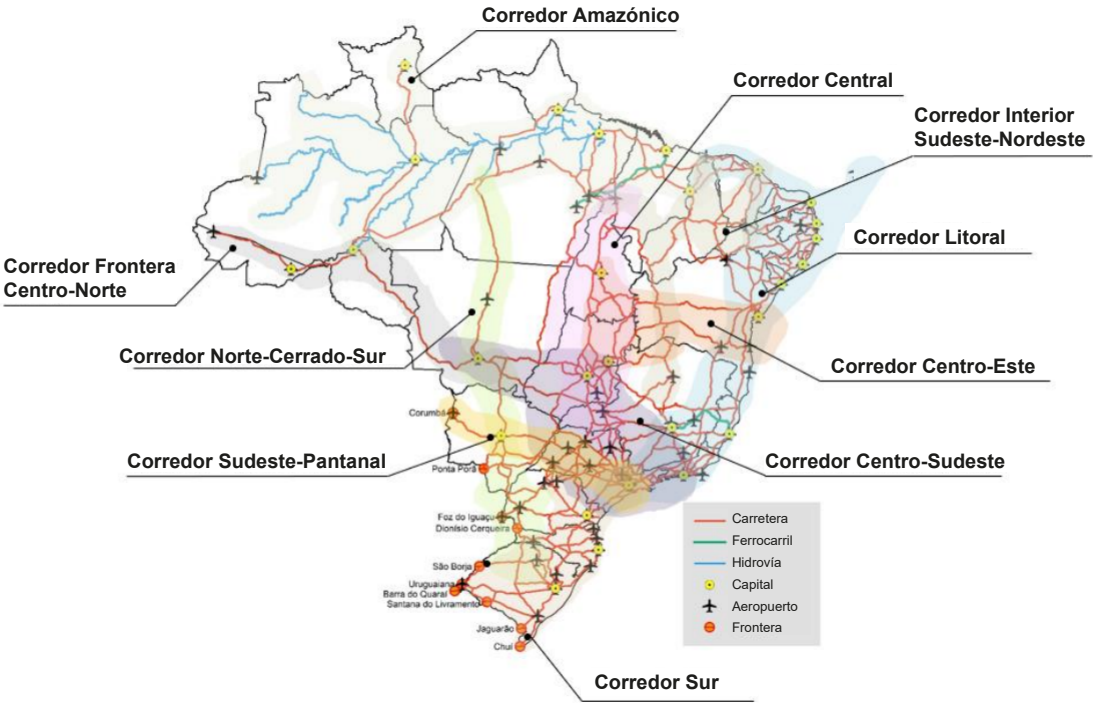
La Ley Federal nº 12.379 (Brasil, 2011) estableció que el Sistema Nacional de Vialidad (SNV) constituye el conjunto de la infraestructura de transporte, pública y privada, responsable de la circulación de personas y mercancías en todo el territorio brasileño. Compuesto por los modos de transporte federal, estatal y municipal por carretera, ferrocarril, agua y aire, sus objetivos son facilitar el desplazamiento eficiente de cargas y pasajeros entre los estados y regiones del país, promover la cohesión territorial y el desarrollo económico sostenible, atender los grandes flujos de mercancías mediante los Corredores Logísticos Estratégicos (CLE), y garantizar la red viaria estratégica necesaria para la seguridad del territorio nacional.

Los Corredores Logísticos Estratégicos (CLE) son ejes que proporcionan inversiones y la creación de mercados, impulsando el desarrollo económico y social. Incluyen un sistema viario formado por diferentes modos que facilitan el transporte eficiente de cargas y, en consecuencia, de personas.

El Proyecto "Corredores Logísticos Estratégicos", realizado por el Ministerio de Transportes entre 2017 y 2020 (Brasil, 2024), como complemento de la Ley nº 12.379, tuvo el objetivo de presentar una visión panorámica y diagnóstica de la infraestructura para el flujo logístico de las principales cargas del país, además de tratar de temas y lugares estratégicos donde el Gobierno actúa promoviendo la infraestructura, como el transporte de pasajeros, la integración y la defensa nacional. El estudio identificó 10 (diez) CLE en Brasil, como se muestra en la Figura 2.

Comparando la definición de ICT, presentada al inicio de este estudio, con la de CLE, se puede afirmar que el SNV puede representar la ICT de Brasil.

Figura 2. CLE en Brasil



Fuente: Brasil (2024).

2.4 Gestión y mitigación de riesgos

La seguridad de las IC se puede definir como la reducción del riesgo de invasiones, ataques o efectos de desastres naturales o antrópicos mediante la aplicación de medios físicos o de medidas cibernéticas defensivas (Estados Unidos de América, 2019). Una estrategia de seguridad de IC debe identificar qué elementos de la infraestructura son críticos para su funcionamiento o representan el mayor peligro para la vida y la propiedad, aunque algunos elementos pueden ser más críticos que otros (Moteff y colaboradores, 2003).

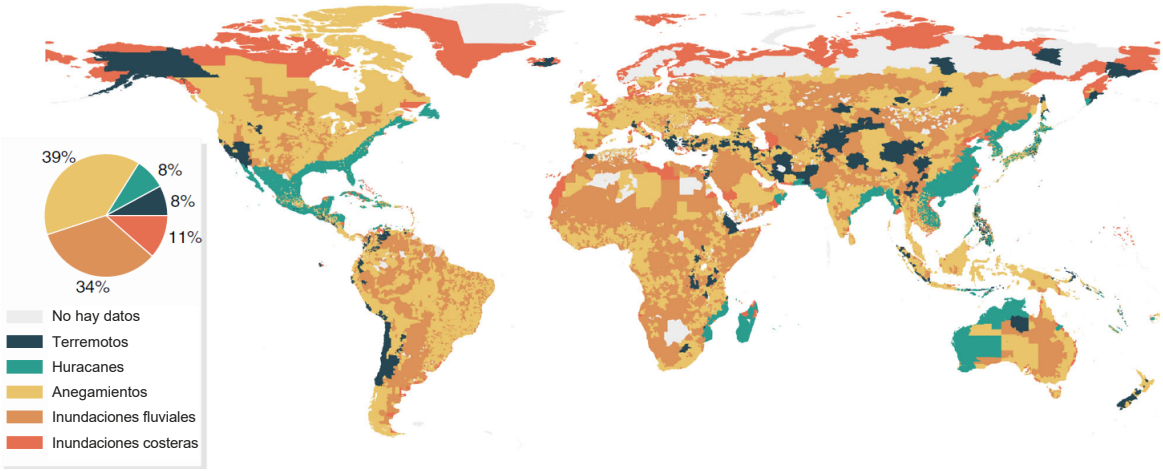
Pero ¿cómo se define riesgo?

CISA (Estados Unidos de América, 2019) define riesgo como el potencial de materialización de un resultado no deseado resultante de un incidente, accidente o evento determinado por su probabilidad y por las consecuencias asociadas. Mientras que la gestión de riesgo es el proceso de identificar, analizar y comunicar, que incluye decidir aceptarlo, evitarlo, transferirlo o controlarlo a un nivel aceptable, dedicando recursos a acciones destinadas a prevenir o mitigar los efectos de amenazas y peligros con una mayor probabilidad de provocar resultados no deseados significativos en una infraestructura.

Moteff y colaboradores (2003) explican que el tamaño y la complejidad de algunas infraestructuras, como carreteras y ferrocarriles de extensión continental, pueden dificultar la identificación de riesgos en elementos individuales de una IC, volviéndola una tarea compleja.

Sin embargo, en un estudio realizado por Koks y colaboradores (2019), se observó que anegamientos (el 39%) e inundaciones fluviales (el 34%) son los factores con mayores niveles de riesgo predominante para las infraestructuras de transporte en la mayoría de los países y regiones del planeta. Específicamente en Brasil, se nota que, como se muestra en la Figura 3, los riesgos a los que está expuesta la ICT nacional se concentran totalmente en estos dos fenómenos climáticos.

Figura 3. Indicación del riesgo predominante para la Infraestructura Crítica de Transporte en cada región



Fuente: Koks y colaboradores (2019).

Mattsson y Jenelius (2015) también observaron que la interrupción de vías, el aislamiento provocado por inundaciones y la frecuencia de lluvias intensas tienen un impacto significativo en el funcionamiento de las redes viarias, así como en las ferroviarias, que son particularmente vulnerables a los riesgos naturales debido a la falta de capacidad excedente[1], a las limitadas opciones de redireccionamiento de trenes y a la presencia de líneas ferroviarias únicas.

También según Koks y colaboradores (2019), se puede mitigar hasta un 42% las estimaciones globales de riesgo de todo tipo de anegamientos e inundaciones mediante la ejecución de obras que adapten los parámetros de drenaje vial. Es decir, adaptar el estándar de las carreteras para que resistan a lluvias intensas con un Período de Retorno (T_r)[2] dos veces mayor, de 100 años en lugar de 50 años, por ejemplo, podría reducir a la mitad los riesgos relacionados con las lluvias intensas, lo que resultaría en una reducción estimada de los costos globales de mantenimiento entre el 0,1% y el 0,9%.

La gestión de riesgos, combinada con la implementación de un método lógico para establecer contextos, identificar, evaluar y tratar riesgos de todo tipo de forma sistémica, desempeña un papel crucial en la seguridad de la ICT, garantizando la capacidad máxima de cada medida de protección y la continuidad de las actividades de transporte y del flujo logístico (Brasil, 2022).

1 Capacidad excedente: infraestructura de soporte instalada y no utilizada, total o parcialmente, disponible para compartir (BRASIL, 2017a).

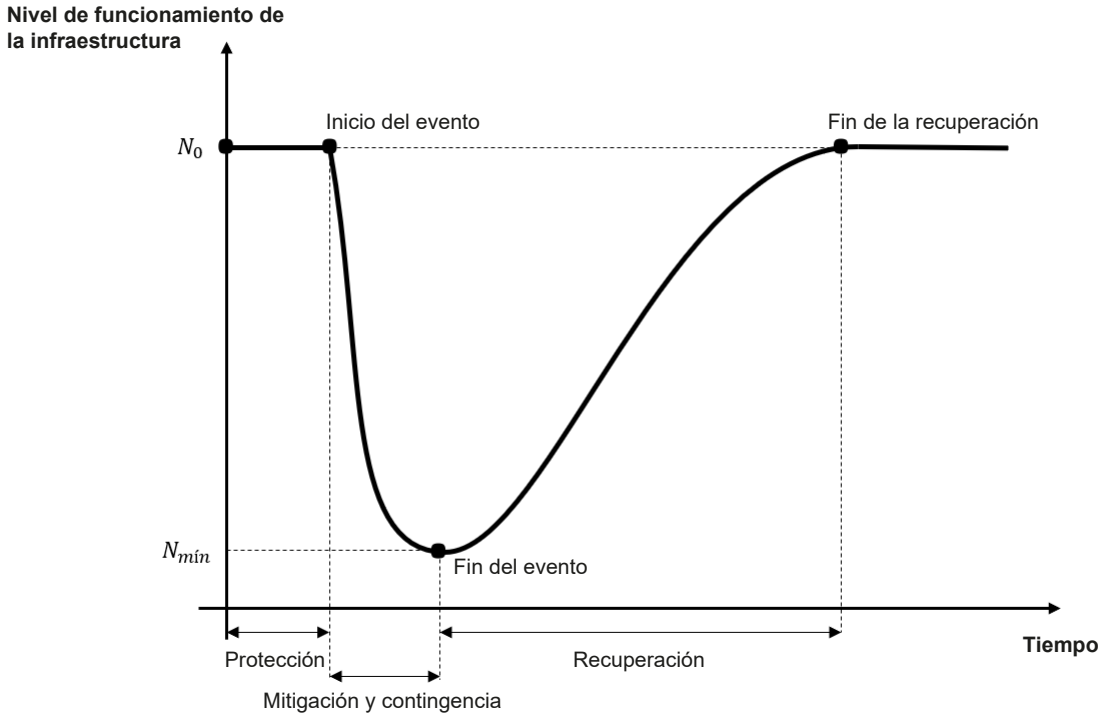
2 Período de retorno (T_r) es el intervalo de tiempo promedio en el que un determinado evento de lluvia es igualado o superado al menos una vez. Cuanto menor el período de retorno, más frecuente y probable es el evento.

2.5 Resiliencia y seguridad de la ICT brasileña

La OCDE (2019) señala que hasta mediados de la década de 2000, las políticas y actividades relacionadas con la seguridad de las IC en todo el mundo se centraban simplemente en proteger los activos. Sin embargo, debido al creciente costo de reparación de desastres o ataques, como los ataques terroristas del 11 de septiembre de 2001 en Estados Unidos, y a los ciberataques dirigidos contra las IC, los gobiernos empezaron a centrarse más en la resiliencia de las estructuras que en su protección.

En momentos de crisis, dedicar esfuerzos exclusivamente a las actividades de protección puede no ser suficiente para garantizar la seguridad de las infraestructuras. En estas situaciones, hay que implementar medidas de mitigación y contingencia para recuperar el sistema desde su nivel de funcionamiento mínimo hasta el nivel anterior al evento de materialización de los riesgos, en el menor tiempo posible, teniendo en cuenta la gravedad de la situación y la criticidad de la estructura (Figura 4). El equilibrio entre las acciones de protección y la gestión de riesgos es fundamental para el éxito de la seguridad de las infraestructuras críticas (Brasil, 2022).

Figura 4. Cambio en el nivel de funcionamiento de una infraestructura provocado por un evento o ataque, y su recuperación gracias a la resiliencia



Fuente: Adaptado de Arrighi, Pregnolato y Castelli (2021).

En Brasil, la PNSIC (Brasil, 2018a) establece que la seguridad de las IC consiste en un conjunto de medidas preventivas y reactivas que tienen el objetivo de preservar o restablecer la prestación de los servicios relacionados con estas infraestructuras; a la vez, la ENSIC (Brasil, 2020)

subraya la importancia de la seguridad de las IC como una actividad fundamental para fortalecer la seguridad y la resiliencia de los sectores estratégicos vitales para el funcionamiento de los Estados, tanto de forma individual como en conjunto.

Una infraestructura resiliente es capaz de resistir y recuperarse rápidamente de interrupciones, ataques intencionales, accidentes, amenazas o incidentes naturales (Estados Unidos de América, 2019). Para Liu y Song (2020), resiliencia se refiere a la capacidad de adaptarse a condiciones en cambio continuo, resistir y recuperarse de interrupciones provocadas por emergencias en el menor tiempo posible. Argyroudis y colaboradores (2020) definen la resiliencia como la propiedad emergente o los atributos que tiene la infraestructura que la permiten soportar, reaccionar y/o adaptarse a una gran variedad de eventos perturbadores mientras mantiene y/o mejora su funcionalidad.

Como observado por Mattsson y Jenelius (2015) y por Koks y colaboradores (2019), la resiliencia de la ICT está íntimamente ligada a su capacidad de adaptarse a las consecuencias de las lluvias intensas. En los casos de construcción de carreteras o de mantenimiento de carreteras vecinales, se estima que adaptar el sistema de drenaje para una frecuencia pluviométrica mayor o para reducir a la mitad los daños financieros esperados, genere un impacto financiero de aproximadamente un 2% en el presupuesto. Sin embargo, para carreteras pavimentadas existentes, redimensionar los parámetros de lluvia implicaría reconstruir secciones enteras de la carretera solamente para reemplazar las tuberías de drenaje (Koks y colaboradores, 2019).

2.6 El Sistema de Ingeniería del Ejército Brasileño

Desde la Guerra del Paraguay, la Ingeniería del Ejército Brasileño ha sido utilizada en obras de ferrocarriles, líneas telegráficas estratégicas y en otros proyectos de interés del Estado. Aunque las empresas privadas han ganado cada vez más espacio en la construcción de infraestructuras tras el final del siglo XIX, la Ingeniería Militar siguió desempeñando un papel importante en emprendimientos estratégicos, principalmente en la construcción de ejes viarios y ferroviarios, fortificaciones permanentes y en el mapeo del territorio (Figueiredo y colaboradores, 2014).

El Manual *A Engenharia nas Operações* (La Ingeniería en las Operaciones) (Brasil, 2018b, p. 2-1) define Ingeniería como el arma de apoyo al combate cuya misión principal es apoyar las operaciones ejecutadas por el Ejército Brasileño, mediante actividades de movilidad, contramovilidad, protección y de apoyo general de ingeniería. Estas acciones tienen el objetivo de multiplicar el poder de combate de las fuerzas amigas y destruir, neutralizar o reducir el poder de combate del enemigo, propiciando la conquista y el mantenimiento de los objetivos establecidos.

Específicamente en la función movilidad, se agrupan tareas desarrolladas para proporcionar el movimiento continuo y constante de una fuerza amiga o de los propios ciudadanos, en tiempos de paz, y está formada, además de otras acciones centradas en el ejercicio de la actividad militar, por trasposición de cursos de agua, y de conservación y reparación de pistas y carreteras. En la misión de apoyo general de ingeniería, la Ingeniería realiza, por ejemplo: la construcción de instalaciones logísticas; la recuperación de áreas dañadas; la construcción, mejora y reparación de hidrovías, carreteras, ferrocarriles y aeródromos.

> Actúa en la función logística ingeniería definida como: 'Conjunto de actividades que se ejecutan con el objetivo de planificar y ejecutar obras y servicios para obtener y adaptar la infraestructura física y las instalaciones existentes a las necesidades de las fuerzas (Brasil, 2018b, p. 2-1).

El Manual *A Engenharia nas Operações* (Brasil, 2018b, p. 2-1) también menciona que las operaciones de Ingeniería en áreas construidas, como en el entorno urbano, se realizan con el objetivo de contribuir al desarrollo nacional en tiempos de paz. Entre los factores que influyen en la defensa de estas áreas están el interés en mantener la posición, las posibilidades que ofrece el lugar y, ante todo, el estado de la infraestructura viaria o ferroviaria para que se pueda llegar al lugar de interés, siendo este el factor principal. En tiempos de guerra, tienen el objetivo de mantener el control parcial o total de la zona para negarla al enemigo, y para garantizar a las fuerzas amigas el control total de las IC a través de la planificación adecuada.

El Departamento de Ingeniería y Construcción (DEC) es el organismo de dirección sectorial del Ejército Brasileño responsable de garantizar y regular el uso del Sistema de Ingeniería del Ejército Brasileño (SEEx) en beneficio del Estado Brasileño. El DEC, mediante el SEEx, desempeña diversas actividades que van desde el mantenimiento de la transitabilidad de carreteras vecinales hasta el montaje de emergencia de puentes desmontables en situaciones de calamidad pública, abarcando la coordinación y la ejecución de obras y servicios de ingeniería de infraestructura física en todo el territorio nacional, en diferentes momentos y regiones, desde el Sur hasta la Amazonía (Brasil, 2021).

Dutra (2017) explica que el Sistema de Ingeniería del Ejército (SEEx) es el instrumento que DEC utiliza para articularse estratégicamente en todo el territorio nacional, tanto en apoyo a las operaciones militares asignadas a la Fuerza Terrestre como al desarrollo nacional, con las siguientes atribuciones:

- ejecutar las actividades relacionadas con el análisis, el estudio de viabilidad técnica y el control de proyectos de ingeniería a través del Sistema de Proyectos de Ingeniería (SPE);
- proyectar, contratar y supervisar obras y servicios diversos de ingeniería en organizaciones militares a través del Sistema de Obras Militares (SOM);
- ejecutar obras y servicios de ingeniería de infraestructura física en cooperación con otros organismos gubernamentales a través del Sistema de Obras de Cooperación (SOC);
- realizar la adquisición, control del acervo y vida útil, uso, descarga y alienación de los materiales de Ingeniería a través del Sistema de Material de Ingeniería (SME); y
- preservar el Medio Ambiente y controlar el patrimonio inmobiliario bajo jurisdicción del Ejército Brasileño a través del Sistema de Patrimonio Inmobiliario y Medio Ambiente (SPIMA).

En cooperación con el Ministerio de Infraestructura, el Departamento Nacional de Ferrocarriles (DNEF), el Departamento Nacional de Carreteras (DNER), e institución sucesora, el Departamento Nacional de Infraestructura de Transporte (DNIT) y otros organismos federales, el SEEx ejecutó diversas obras de grandes ejes viarios y ferroviarios, además de construir puertos y aeropuertos en todo el territorio nacional. En el Norte y el Nordeste, entre las décadas de 1950 y 1970, ejecutó obras de implantación y construcción de carreteras, como el inicio de la implantación de los 4.918 km de la BR-230, conocida como Transamazónica, y los

1.114 km de la BR-116, con el objetivo de conectar las principales ciudades de la región, mitigar los impactos de la devastadora sequía en la región semiárida y, como consecuencia, promover el desarrollo regional.

Más tarde, en la década de 1990, los esfuerzos se intensificaron en la conservación y restauración de carreteras federales, como la restauración de 196 km de la BR-319 entre Porto Velho y el límite entre Amapá y Roraima. En el sector de ferrocarriles, el Sistema actuó en diversas obras de extrema importancia, como: la implantación del ferrocarril Paraná-Mato Grosso en 1901; la conexión entre Uberlândia y Brasilia y la construcción de 60 km de ferrocarril para conectar Piripiri y Teresina en la década de 1960. En 1950, el 1º Batallón de Ferrocarriles fue el responsable de construir el ferrocarril de Tronco Principal Sur, en el tramo que abarcaba desde el Río Canoas hasta el Río Pelotas (Figueiredo y colaboradores, 2014).

Dutra (2017) explica que a principios de este siglo hubo un significativo aumento de recursos resultante de las inversiones realizadas y la diversificación de aliados del Ejército Brasileño, principalmente del esfuerzo realizado por el DEC para establecer nuevas alianzas con otros organismos gubernamentales. Esto permitió recuperar equipos y vehículos, así como reanudar la capacitación del personal militar y civil tras un hiato intelectual de décadas.

Las consecuencias de esta decisión resultaron en beneficios significativos para el SEEx, que actualmente cuenta con tropas de ingeniería capacitadas y listas para ser utilizadas en misiones en pro del desarrollo nacional, integrar Fuerzas de Paz o apoyar la Defensa Civil, además de resultar en un gran acervo de obras de infraestructura de transporte para el Ejército Brasileño (Tabla 3).

Tabla 3. Acervo de obras de infraestructura de transporte ejecutadas por el SEEx entre 1901 y 2017

Acervo de obras de infraestructura de transporte ejecutadas por el SEEx		
Descripción	**Unidad**	**Cantidad**
Carreteras (construcción, pavimentación y carreteras vecinales)	km	26.900
Ferrocarriles	km	5.800
Aeropuertos	un	13
Puentes y Viaductos	m	58.500
Túneles	m	47.500
Puertos	un	3

Fuente: Dutra (2017).

En septiembre de 2020, el DEC y *Valec Engenharia, Construções e Ferrovias S.A.* (Valec Ingeniería, Construcciones y Ferrocarriles Sociedad Anónima), una empresa pública vinculada al Ministerio de Infraestructura cuya función es construir y explorar la infraestructura ferroviaria, firmaron un Término de Ejecución Descentralizada con el objetivo de ejecutar 18,34 km del Ferrocarril de Integración Oeste-Este (FIOL). La motivación para el instrumento surge del interés recíproco en un régimen de colaboración mutua entre las partes involucradas, con el objetivo de contribuir a un mayor equilibrio de la matriz de transporte de carga de Brasil, el flujo de la producción y la mejora de la calidad de vida de la población (DEC, 2020). La alianza también simboliza el retorno del SEEx a las actividades de construcción ferroviaria.

3 LA SEGURIDAD DE LA ICT DESDE LA PERSPECTIVA DEL SEEX

En los Objetivos Nacionales de Defensa de la PND, se señalan las IC, entre ellas la ICT por proporcionar la Capacidad de Movilidad Estratégica (Brasil, 2023, p. 38), como factores de soporte a las Fuerzas Armadas para supervisar, controlar y defender el territorio (Brasil, 2023, p. 24), lo que proporciona al Ejército Brasileño la capacidad de hacerse presente en todo el territorio nacional (Brasil, 2023, p. 51).

Mientras la revisión de la PND establece una relación de dependencia entre las Fuerzas Armadas y la ICT, la revisión de la END invierte esta relación, asignando de forma clara y objetiva al Ejército Brasileño la responsabilidad de la seguridad, específicamente de la protección, de las IC valiéndose de las actividades realizadas por el SEEx:

> Como consecuencia de la estrategia de la presencia, **el Ejército** [...]. **Participará, además, en la protección integrada de Estructuras Críticas y en la ejecución de obras de ingeniería en todo el territorio nacional**, en beneficio del desarrollo del País (Brasil, 2023, p. 54, énfasis agregado por el autor).

Y complementa la atribución de responsabilidad a las Fuerzas Armadas de contribuir a la seguridad de la ICT en la Estrategia para Fortalecer el Poder Nacional, dentro del Objetivo Nacional de Garantizar la soberanía, el patrimonio nacional y la integridad territorial, y el Objetivo de Aumentar la proyección de Brasil en el concierto de las naciones y su inclusión en procesos decisorios internacionales:

> AED-2 **Contribuir al aumento del nivel de seguridad de las Estructuras Críticas** de sistemas de captación, tratamiento y distribución de agua; generación y distribución de energía eléctrica; **transporte**; producción y distribución de combustibles; y comunicaciones, entre otros (Brasil, 2023, p. 63 y 73, énfasis agregado por el autor).

Además de las disposiciones legales establecidas en la Política Nacional de Defensa y en la Estrategia Nacional de Defensa, la Ley Complementaria nº 97 (Brasil, 1999) establece, en su artículo 16, la atribución subsidiaria general de las Fuerzas Armadas de colaborar con el desarrollo nacional y la defensa civil. Del mismo modo, el artículo 17, apartado A, establece la atribución específica del Ejército Brasileño de cooperar con organismos públicos federales, estatales y municipales, así como, en situaciones extraordinarias, con empresas privadas, en la ejecución de obras y servicios de ingeniería.

El Plansic (Brasil, 2022), al distribuir las responsabilidades entre los Ministerios para la elaboración de los Planes Sectoriales de seguridad de IC, consideró el Ministerio de Infraestructura como el responsable de implementar las acciones estratégicas y elaborar los planes relativos a la ICT. En el mismo documento, para complementar, se abre la posibilidad de que otros organismos y entidades públicos y privados con conocimientos en la protección de las IC participen en la elaboración y desarrollo de planes específicos.

Observando lo expresado literalmente en las PND/END (Brasil, 2023) sobre el papel del Ejército Brasileño en la protección y la seguridad de las IC nacionales, se puede clasificar la

institución como poseedora de los conocimientos específicos necesarios para actuar con el Ministerio de Infraestructura en el desempeño de sus actividades relacionadas con la seguridad de la ICT.

4 CONSIDERACIONES FINALES

Ninguna de las definiciones sobre lo que constituye una IC, según se constató en la revisión bibliográfica, se puede considerar rigurosa. La literatura presenta ciertas limitaciones, pero ofrece margen de interpretación en cuanto a las infraestructuras que se ajustan a esta definición. Esencialmente, el desafío que enfrentan los gobiernos nacionales es identificar y reducir el impacto esperado sobre las IC ante cualquier tipo de riesgo o amenaza.

En el caso de los países que integran la OCDE, como EE.UU. y países de la Unión Europea, como están más expuestos a amenazas terroristas, los instrumentos de seguridad de IC alcanzan un mayor nivel de madurez en comparación con los de Brasil, incluso con la participación de entidades centradas exclusivamente en la protección y gestión de riesgos, como CISA en EE.UU. y CPNI en Reino Unido.

Al observar la ICT, se nota que prácticamente todos los países analizados en el estudio sobre la clasificación de sectores esenciales definieron que se considera el sector de transportes una IC debido a su papel fundamental que desempeña en el funcionamiento de la cadena logística de diversos servicios esenciales para la sociedad. La sociedad, en cualquier nivel, no solo cuenta con la infraestructura de transportes, principalmente con la red de carreteras, para la movilidad diaria y el transporte de bienes y servicios, sino también como un sistema auxiliar para el rescate y salvamento de personas y activos, además de permitir acciones de emergencia o reparación en otras infraestructuras afectadas por eventos adversos.

El vasto territorio brasileño y la diversidad de sus actividades productivas exigen una infraestructura eficiente e integral. El transporte de pasajeros permite la movilidad de la fuerza laboral y promueve la integración entre las diferentes regiones, lo que también impulsa el turismo, mientras que el transporte de cargas es responsable de distribuir los insumos necesarios para la producción y el flujo de insumos y productos, conectando productores, industrias y consumidores en un complejo sistema logístico.

Desde la perspectiva de la gestión y mitigación de riesgos, se pudo observar que el fenómeno climático de lluvias intensas es el responsable de todas las amenazas predominantes a las que está expuesta la ICT brasileña. Sin embargo, las acciones que tienen el objetivo de aumentar la protección y la resiliencia de las infraestructuras, como las obras de adaptación de los parámetros de drenaje, pueden reducir casi a la mitad los riesgos de anegamientos e inundaciones, lo que reduciría hasta un 0,9% de los costos globales de mantenimiento. Desde el punto de vista de la aplicación de medidas no estructurales[3], políticas públicas integrales también pueden limitar el riesgo de interrupciones en los servicios de transporte esenciales y aumentar la capacidad de recuperación rápida tras un impacto.

Los instrumentos legales para la defensa nacional, consolidados en los niveles político y estratégico mediante las PND/END (Brasil, 2023), abren espacio para que el Ejército Brasileño

3 Las medidas no estructurales son las que no implican la ejecución de obras o servicios de ingeniería. Pueden ser políticas públicas, como campañas de concienciación, por ejemplo.

actúe en la seguridad de la ICT a través del uso de mecanismos a nivel táctico que pueden, incluso, respaldar la elaboración del Plan Sectorial de transportes previsto en el Plansic.

La atribución complementaria (Brasil, 1999) también permitió a la institución, específicamente al SEEx, ejecutar obras y servicios de ingeniería en todo el territorio nacional, incluso mediante alianzas con empresas privadas y otros organismos gubernamentales, lo que desencadenó la construcción de una infraestructura de transporte terrestre equivalente al tamaño de la red ferroviaria suiza (CIA, 2023a) y la red viaria croata (CIA, 2023b).

Sabiendo que el DEC es el único organismo de la administración pública federal capaz de realizar obras de infraestructura mediante ejecución directa, y mirando el extenso acervo de obras exitosas realizadas a lo largo de más de un siglo por el SEEx, sería un error estratégico que los Ministerios responsables de implementar, mantener y desarrollar infraestructuras de transporte, como el Ministerio de Infraestructura, no solicitaran el apoyo del Ejército Brasileño, a través del Ministerio de Defensa, en la participación en el Plan Sectorial de la ICT.

En el análisis de la relación entre las Fuerzas Armadas, más específicamente el Ejército Brasileño, y la infraestructura de transporte brasileña en las PND/END (Brasil, 2023), se puede observar que existe una relación causal cíclica (Figura 5) entre las misiones constitucionales y complementarias de la Fuerza Terrestre y la seguridad de la ICT, visto que, mientras las Fuerzas dependen de la plena disponibilidad de las redes viarias y ferroviarias para garantizar la Capacidad de Movilidad Estratégica, el Ejército, a su vez, debe proporcionar la seguridad de las estructuras críticas existentes, además de ejecutar nuevas obras en todo el territorio brasileño, colaborando con el desarrollo nacional y la defensa civil (Brasil, 1999).

Figura 5. Relación cíclica de causa y efecto entre la ICT y el Ejército Brasileño

Fuente: elaborado por el autor.

Al comparar los mecanismos de seguridad de IC brasileños con los de EE.UU. y Unión Europea, se puede observar que aún queda un largo camino por recorrer para alcanzar un nivel adecuado de gestión y mitigación de riesgos. Sin embargo, la falta de una legislación a nivel táctico específica para la seguridad de la ICT no evitó que el Sistema de Ingeniería del Ejército Brasileño

siempre estuviera capacitado para actuar proyectando, ejecutando y supervisando las obras de construcción y mantenimiento de infraestructuras de transporte en diversos ambientes y regiones.

Aunque no está expuesta a la inminencia de ataques terroristas o de enemigos, la sociedad brasileña debe ser consciente de los riesgos a los que está expuesta, principalmente a los riesgos relacionados con las lluvias intensas, porque son las responsables de todas las amenazas predominantes a la ICT.

Este artículo, aunque ha profundizado en un tema poco discutido en la literatura nacional, se limitó a estudiar las relaciones del SEEx con la seguridad de tipos restringidos de infraestructuras de transportes, como las estructuras físicas de carreteras y ferrocarriles. Como mencionado en la introducción, la ICT de un país también puede abarcar las estructuras físicas de puertos y aeropuertos y el sistema de transporte de pasajeros. Dicho esto, se sugiere que estudios futuros traten de la relación del SEEx con la seguridad de otros activos que componen la ICT brasileña, y también recomienda que, tras elaborar el Plan Sectorial de seguridad para el sector de transporte, se reevalúe la actuación del SEEx ante las metas establecidas. También se recomienda que se estudie la actuación del SEEx en el mantenimiento de la integridad de la IC del país, presentando la recopilación de datos históricos y la evaluación del desempeño del Sistema, utilizando preferentemente métodos de análisis socioeconómico de programas y proyectos.

Finalmente, se concluye que el SEEx ha colaborado con la seguridad de la ICT brasileña de una manera objetiva al actuar en la gestión y mitigación de los riesgos mediante la ejecución de obras y servicios de ingeniería, lo que proporciona una mayor resiliencia a las infraestructuras físicas terrestres.

REFERENCIAS

ARGYROUDIS, Sotirios; MITOULIS, Stergios; HOFER, Lorenzo; ZANINI, Mariano; TUBALDI, Enrico; FRANGOPOL, Dan. Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. **Science of the Total Environment**, [*s. l.*], v. 714, 136854, 2020.

ARRIGHI, Chiara; PREGNOLATO, Maria; CASTELLI, Fabio. Indirect flood impacts and cascade risk across interdependent linear infrastructures. **Natural Hazards and Earth System Sciences**, [*s. l.*], n. 21, p. 1955-1969, 2021.

BRASIL. **Resolução nº 683, de 05 de outubro de 2017**. Aprova o Regulamento de Compartilhamento de Infraestrutura de Suporte à Prestação de Serviço de Telecomunicações. Brasília, DF: Presidência da República, 2017a.

BRASIL. **Decreto nº 9.573, de 22 de novembro de 2018**. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 22 nov. 2018a.

BRASIL. EXÉRCITO BRASILEIRO. **A Engenharia nas Operações**. EB70-MC-10.237. 1. ed. Brasília, DF: Ministério da Defesa, DF: Presidência da República, 2018b.

BRASIL. EXÉRCITO BRASILEIRO. **Regulamento do Departamento de Engenharia e Construção**. EB10-R-04.001. Brasília, DF: Ministério da Defesa, 2021.

BRASIL. EXÉRCITO BRASILEIRO. **Manual de Campanha - Operações**. EB70-MC-10.223. 5. ed. Brasília, DF: Ministério da Defesa, 2017b.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, DF: Presidência da República, 2008.

BRASIL. **Decreto nº 10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 9 dez. 2020.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República, 15 set. 2022.

BRASIL. **Lei Complementar nº 97, de 9 de junho de 1999**. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, DF: Presidência da República, 9 jun. 1999.

BRASIL. **Lei nº 12.379, de 6 de janeiro de 2011**. Dispõe sobre o Sistema Nacional de Viação - SNV. Brasília, DF: Presidência da República, 6 jan. 2011.

BRASIL. MINISTÉRIO DOS TRANSPORTES. **Corredores Logísticos Estratégicos**. Brasília: Ministério dos Transportes. DF: Ministério dos Transportes, 2024. Disponível em: https://www.gov.br/transportes/pt-br/assuntos/PIT/politica-e-planejamento/cle. Acesso em 13 fev. 2025.

BRASIL. **Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END)**: encaminhadas, em 22 de julho de 2020, para apreciação do Congresso Nacional. Brasília, DF: Presidência da República, 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 6 jun. 2023.

CÂMARA aprova atualização da Política Nacional de Defesa. **Agência Câmara de Notícias**, Brasília, DF, 15 maio 2024. Disponível em: https://www.camara.leg.br/noticias/1062814-CAMARA-APROVA-ATUALIZACAO-DA-POLITICA-NACIONAL-DE-DEFESA. Acesso em: 4 fev. 2025.

CIA - CENTRAL INTELLIGENCE AGENCY. **Country Comparisons – Railways**. Disponível em: https://www.cia.gov/the-world-factbook/field/railways/country-comparison. Acesso em 24 jun. 2023a.

CIA - CENTRAL INTELLIGENCE AGENCY. **Country Comparisons – Roadways**. Disponível em: https://www.cia.gov/the-world-factbook/field/roadways/country-comparison. Acesso em 24 jun. 2023b.

DEC - DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO. **Termo de Execução Descentralizada - TED Nº 001/2020**. Brasília, DF, 08 set. 2020. Disponível em: http://www.dec.eb.mil.br/images/PERMANENTE/TED/SEI_MINFRA_-_2769928_-_TED_001-2020-assinado.pdf. Acesso em: 19 jun. 2023.

DUTRA, Antônio. **A institucionalização da participação do Sistema de Obras de Cooperação do Exército Brasileiro em serviços de infraestrutura no país – uma proposta**. 2017. 59 f. Trabalho de Conclusão de Curso – Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia, Rio de Janeiro, 2017.

ESTADOS UNIDOS DA AMÉRICA. Cybersecurity and Infrastructure Security Agency (CISA). **A Guide to Critical Infrastructure Security and Resilience**. Washington, DC, 2019.

ESTADOS UNIDOS DA AMÉRICA. Cybersecurity and Infrastructure Security Agency (CISA). **Infrastructure Security**. Disponível em: https://www.cisa.gov/infrastructure-security. Acesso em: 6 jun. 2023.

FIGUEIREDO, Washington; OLIVEIRA, Emerson; SANTANA, José; ALVES, Edmar. **A engenharia do exército na construção do desenvolvimento nacional**. Brasília, DF: Departamento de Engenharia e Construção, 2014. 294 p.

INTERNATIONAL STANDARDS ORGANIZATION (ISO). **ISO 3166**: codes for the representation of names of countries. 4. ed. Genebra: [*s. n.*], 2020.

KOKS, E.; ROZENBERG, J.; ZORN, C.; TARIVERDI, M.; VOUSDOUKAS, M.; FRASER, S.; HALL, J.; HALLEGATTE, S. A global multi-hazard risk analysis of road and railway. **Nature Communications**, [*s. l.*], v. 10, n. 2677, 2019.

LIU, Wei; SONG. Zhaoyang. Review of studies on the resilience of urban critical infrastructure networks. **Reliability Engineering and System Safety**, [*s. l.*], v. 2020, n. 193, 2019.

MATTSSON, Lars-Göran; JENELIUS, Erik. Vulnerability and resilience of transport systems – A discussion of recent research. **Transportation Research Part A**, [*s. l.*], v. 81, p 16-34, 2015.

MOTEFF, John; COPELAND, Claudia; FISCHER, John. Critical Infrastructures: **What Makes an Infrastructure Critical?** Congressional Research Service – The Library of Congress. EUA, 29 jan. 2003. Disponível em: https://irp.fas.org/crs/RL31556.pdf. Acesso em: 25 jun. 2023.

NATÁRIO, Rui; NUNES, Paulo. Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. **Revista Militar**, Lisboa, n. 2547, p 249-286, 2014.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OCDE). **Good Governance for Critical Infrastructure Resilience**. OECD Reviews of Risk Management Policies. Paris: OECD Publishing, 2019

PAIVA, Iure. Política Nacional de Defesa e proteção da infraestrutura energética crítica no Brasil. **Austral: Revista Brasileira de Estratégia e Relações Internacionais**, [*s. l.*], v. 5, n. 10, 2016.

POLÍTICA Nacional de Defesa é aprovada no Senado e segue para Câmara. **Agência Senado**, Brasília, DF, 22 junho 2022. Disponível em: https://www12.senado.leg.br/noticias/noticias/materias/2022/06/02/politica-nacional-de-defesa-e-aprovada-no-senado-e-segue-para-camara. Acesso em: 25 jun. 2023.

REINO UNIDO. Centre for the Protection of National Infrastructure (CPNI). **Critical National Infrastructure**. Disponível em: https://www.cpni.gov.uk/critical-national-infrastructure-0. Acesso em: 6 jun. 2023.

ROCHA, Paulo Cesar. **A relação entre a gestão de riscos integrada em uma organização com infraestrutura crítica e as questões de Defesa Nacional**. 2019. Trabalho de Conclusão de Curso (Curso de Altos Estudos em Defesa) - Escola Superior de Guerra, Brasília, DF, 2019.