

INFRAESTRUCTURAS CRÍTICAS EN REPÚBLICA DOMINICANA: ANÁLISIS JURÍDICO COMPARADO CON ESPAÑA

Critical infrastructures in the Dominican Republic: A legal analysis compared with Spain

Recibido: 21/ 07 / 2026 | Revisado: 22 / 08 / 2026 | Aprobado: 11 / 09 / 2026

DOI: <https://doi.org/10.59794/rscd.2026.v12i12.181>



Rubén Guillermo Mejía del Carmen

República Dominicana

Correo: mejiadelcarmen@outlook.com

Orcid: <https://orcid.org/0009-0000-3622-2877>.

El autor es oficial superior de la Fuerza Aérea de República Dominicana, piloto aviador y profesional especializado en seguridad operacional aeronáutica, investigación de accidentes, asuntos internacionales, gestión pública y educación superior. Posee formación como licenciado en Derecho y de posgrado en Diplomacia, Relaciones Internacionales, Seguridad y Defensa, así como en International Business Management. Ha desempeñado funciones de dirección en operaciones

aéreas, defensa aérea, asuntos internacionales, recursos humanos, seguridad operacional aeronáutica, formación académica y cooperación internacional. Docente en la Facultad de Ciencias Aeronáuticas de la Universidad Superior para la Defensa (UNADE) y asesor de tesis de la Maestría en seguridad y Defensa de la UNADE, con una línea de trabajo orientada al fortalecimiento institucional, la resiliencia estratégica y la transferencia de conocimiento.



RESUMEN

El presente artículo analiza la necesidad de fortalecer el marco jurídico e institucional dominicano para la protección de infraestructuras críticas, tomando como referencia el modelo normativo del Reino de España. La investigación se fundamenta en una revisión documental y un análisis jurídico-comparado de normas españolas, dominicanas y europeas vinculadas a servicios esenciales, gestión de riesgos, ciberseguridad, terrorismo y resiliencia institucional. El estudio identifica que la República Dominicana ha avanzado en instrumentos relevantes, especialmente en gestión de riesgos y ciberseguridad; sin embargo, aún no cuenta con una ley marco integral que defina infraestructuras críticas, operadores críticos, sectores estratégicos, catálogo nacional, planes sectoriales, planes de seguridad del operador y mecanismos permanentes de coordinación público-privada. El modelo español ofrece una referencia útil por su estructura normativa, sus instrumentos de planificación y su evolución reciente hacia la resiliencia de entidades críticas. Se concluye que el país requiere una política pública nacional de protección y resiliencia de infraestructuras críticas, articulada con la seguridad nacional, la defensa, la gestión de riesgos, la ciberseguridad y la continuidad de servicios esenciales.

Palabras clave: Infraestructuras críticas, seguridad nacional, resiliencia, ciberseguridad, República Dominicana.

ABSTRACT

This article analyzes the need to strengthen the Dominican legal and institutional framework for the protection of critical infrastructures, taking as a reference the regulatory model of the Kingdom of Spain. The research is based on a documentary review and a legal-comparative analysis of Spanish, Dominican and European regulations related to essential services, risk management, cybersecurity, terrorism and institutional resilience. The study identifies that the Dominican Republic has made progress in relevant instruments, especially in risk management and cybersecurity; however, it does not yet have a comprehensive framework law that defines critical infrastructures, critical operators, strategic sectors, national catalog, sectoral plans, operator security plans and permanent public-private coordination mechanisms. The Spanish model offers a useful reference for its regulatory structure, its planning instruments and its recent evolution towards the resilience of critical entities. It is concluded that the country requires a national public policy for the protection and resilience of critical infrastructures, articulated with national security, defense, risk management, cybersecurity and the continuity of essential services.

Keywords: Critical infrastructures, national security, resilience, cybersecurity, Dominican Republic.



INTRODUCCIÓN

La protección de las infraestructuras críticas constituye una dimensión esencial de la seguridad nacional contemporánea. En sociedades altamente interdependientes, los servicios básicos que permiten la vida social, la actividad económica, el funcionamiento del Estado y la continuidad de las operaciones públicas y privadas descansan sobre instalaciones, redes, sistemas y capacidades cuyo deterioro o interrupción puede generar consecuencias graves para la población. Energía, agua, transporte, salud, telecomunicaciones, finanzas, alimentación, administración pública, seguridad, defensa y sistemas digitales son sectores cuya afectación no se limita al daño físico de una instalación, sino que puede producir efectos en cadena sobre la gobernabilidad, la economía, el orden público y la confianza ciudadana.

En el caso de la República Dominicana, el debate sobre infraestructuras críticas ha estado estrechamente asociado a la ciberseguridad, la gestión de riesgos y la protección de servicios esenciales. La Estrategia Nacional de Ciberseguridad 2030 y los trabajos del Centro Nacional de Ciberseguridad han incorporado la protección y resiliencia de infraestructuras como línea de acción relevante. Sin embargo, el tratamiento normativo sigue siendo fragmentado: existen referencias dispersas en leyes y políticas sobre gestión de riesgos, ciberdelitos, terrorismo, seguridad nacional y ciberseguridad, pero no una ley marco específica que establezca un Sistema Nacional de Protección y Resiliencia de Infraestructuras Críticas. (Baralt Blanco, 2021; Centro Nacional de Ciberseguridad, 2024).

El presente artículo parte de una premisa central: la protección de infraestructuras críticas no debe reducirse a ciberseguridad, aunque la ciberseguridad sea un componente indispensable. Debe abordarse como un sistema jurídico, institucio-

nal, operativo y estratégico que integre gestión de riesgos, defensa, seguridad interior, protección civil, continuidad operativa, cooperación público-privada y resiliencia nacional. Desde esa perspectiva, el modelo español ofrece una referencia comparada útil por su Ley 8/2011, el Real Decreto 704/2011, sus instrumentos de planificación y su evolución reciente hacia la protección y resiliencia de entidades críticas. (Ley 8/2011, 2011; Real Decreto 704/2011, 2011).

El objetivo de este trabajo es analizar la situación normativa dominicana sobre infraestructuras críticas a la luz de la experiencia española, identificar brechas jurídicas e institucionales y proponer lineamientos para una política pública nacional orientada a la protección, continuidad y resiliencia de servicios esenciales. La relevancia del tema es evidente: una nación insular, dependiente de nodos logísticos, puertos, aeropuertos, energía, telecomunicaciones, servicios financieros y sistemas digitales, requiere mecanismos formales para identificar, clasificar, proteger y recuperar aquellas infraestructuras cuya interrupción pueda afectar la seguridad, la economía y el funcionamiento del Estado. El análisis se apoya en revisión documental y comparación jurídico-institucional de normas dominicanas y españolas relacionadas con infraestructuras críticas, servicios esenciales, ciberseguridad, gestión de riesgos y resiliencia nacional.

Desde el punto de vista metodológico, el artículo realiza una comparación jurídico-institucional de carácter documental, descriptivo y aplicado, complementada con un componente exploratorio de campo. La comparación entre España y República Dominicana no se plantea como trasplante automático de normas, sino como contraste funcional de categorías: definición legal de infraestructura crítica y servicio esencial; autoridad competente; sectorización; catálogo o



inventario reservado; obligaciones de operadores; instrumentos de planificación; coordinación público-privada; integración entre seguridad física, ciberseguridad y resiliencia; y mecanismos de seguimiento o evaluación.

El componente empírico utilizado para sustentar las figuras 2 y 3 tiene alcance exploratorio y no pretende representar estadísticamente a todas las instituciones dominicanas. Procede de una encuesta de diez preguntas cerradas aplicada el 27 de septiembre de 2021 a diez participantes vinculados a instituciones llamadas a formar parte de un eventual sistema nacional de protección de infraestructuras críticas, incluyendo personal de las Fuerzas Armadas, CESAC, INDOTEL, IDAC, entre otras instituciones estatales y actores del sector privado. El proce-

dimiento consistió en consultar conocimiento conceptual, percepción sobre legislación existente, pertinencia de adaptar modelos comparados y relación del tema con seguridad y defensa; posteriormente, los resultados fueron convertidos en figuras de apoyo diagnóstico.

La aportación original del trabajo consiste en integrar tres planos que suelen aparecer separados en estudios previos: la revisión jurídico-comparada del modelo español, el diagnóstico de dispersión normativa dominicana y una propuesta gradual de arquitectura institucional para transitar desde un enfoque predominantemente cibernético o de gestión de riesgos hacia un sistema integral de protección y resiliencia de infraestructuras críticas adaptado al contexto dominicano.

DESARROLLO

El análisis de la literatura científica internacional contemporánea pone en relieve que la protección de infraestructuras críticas ha evolucionado desde una posición centrada en activos hacia la medición de resiliencia, la gestión de interdependencias, la continuidad de servicios esenciales y la gobernanza colaborativa. La documentación especializada más reciente destaca indicadores de resiliencia, marcos multicriterio, evaluación de amenazas compuestas y esquemas de asociación público-privada para preparar, absorber, recuperar y adaptar sistemas críticos ante eventos inesperados (Ampratwum et al., 2022; Osei-Kyei et al., 2023; Rathnayaka et al., 2022; Wells et al., 2022; Yang et al., 2023; Yang et al., 2024; Yu et al., 2025). Esta visión refuerza el análisis, ya que permite evaluar no solo la existencia formal de normas, sino también los niveles de proactividad institucional para anticipar fallas diversas, sostener servicios esenciales y restablecer funciones estratégicas después de una crisis.

FUNDAMENTOS CONCEPTUALES DE LAS INFRAESTRUCTURAS CRÍTICAS

La noción de infraestructura crítica surge de la necesidad de proteger aquellos activos, redes o sistemas que sostienen funciones vitales de la sociedad. Aunque cada Estado adapta el concepto a su realidad institucional, existe un núcleo común: una infraestructura se considera crítica cuando su perturbación, destrucción o interrupción puede afectar gravemente la prestación de servicios esenciales, la salud pública, la seguridad, la economía, el orden social o el funcionamiento de las instituciones públicas.

La legislación española ofrece una formulación útil. La Ley 8/2011 distingue entre infraestructuras estratégicas, infraestructuras críticas, servicios esenciales, sectores estratégicos y operadores críticos. Las infraestructuras estratégicas son instalaciones, redes, sistemas y equipos físicos o tecnológicos sobre los que descansa el funcionamiento de servicios esenciales. Las infraestructuras críticas son aquellas infraestructuras estratégicas cuyo fun-



cionamiento es indispensable y no admite soluciones alternativas razonables, de modo que su perturbación o destrucción generaría un grave impacto sobre servicios esenciales. (Ley 8/2011, 2011).

Esta distinción es importante para la República Dominicana. No toda infraestructura estratégica debe clasificarse como crítica. Un aeropuerto, un puerto, una subestación eléctrica, una planta de tratamiento de agua, una red de telecomunicaciones o una plataforma digital estatal puede ser estratégica, pero su criticidad requiere una evaluación técnica basada en impacto, interdependencias, posibilidad de sustitución, tiempo de recuperación y consecuencias sobre la población. La ausencia de criterios homogéneos puede producir dos efectos indeseables: declarar todo como crítico, debilitando la priorización; o declarar muy poco, dejando expuestos sectores esenciales.

EL MODELO ESPAÑOL COMO REFERENCIA NORMATIVA

El Reino de España cuenta con un sistema normativo específico para la protección de infraestructuras críticas. La Ley 8/2011 establece

medidas para proteger infraestructuras críticas frente a amenazas deliberadas de carácter físico y cibernético, así como un sistema organizativo que integra a las Administraciones Públicas y a entidades privadas afectadas. Esta norma resulta relevante para el caso dominicano porque no se limita a declarar principios generales; crea una arquitectura institucional y asigna responsabilidades concretas. (Ley 8/2011, 2011).

Uno de los aspectos más valiosos del modelo español es su sistema de planificación. La Ley 8/2011 contempla el Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales, los Planes de Seguridad del Operador, los Planes de Protección Específicos y los Planes de Apoyo Operativo (ver figura 1). Este conjunto permite traducir la norma en capacidades operativas. No basta con identificar una infraestructura crítica; es necesario definir quién la protege, bajo qué criterios, con qué niveles de seguridad, con qué protocolos, en coordinación con cuáles autoridades y con qué responsabilidades para el operador. (Ley 8/2011, 2011).

Figura 1

Plan Nacional de Protección de Infraestructuras Críticas (PNPIC).



Nota: Adaptación propia con fines de síntesis visual a partir de Vidal López (2017) y del esquema de planificación previsto en la Ley 8/2011 y el Real Decreto 704/2011.



El Real Decreto 704/2011 desarrolla el marco de la Ley 8/2011. Define instrumentos de planificación, procedimientos de aprobación, mecanismos de registro y clasificación, coordinación con operadores críticos y responsabilidades de los órganos del sistema. Su utilidad comparada radica en que convierte la política de protección en un modelo administrativamente ejecutable. La existencia de un catálogo, de planes sectoriales y de obligaciones para operadores crea una cadena de responsabilidad que vincula al Estado con los titulares o gestores de infraestructuras esenciales. (Ley 8/2011, 2011; Real Decreto 704/2011, 2011).

El modelo español también refleja la importancia de la coordinación público-privada. Muchas infraestructuras esenciales son propiedad, administración o gestión de actores privados. Por tanto, el Estado no puede protegerlas mediante un esquema exclusivamente militar, policial o administrativo. Requiere mecanismos legales que obliguen a los operadores críticos a evaluar riesgos, elaborar planes de seguridad, designar responsables, comunicar incidentes, coordinar con autoridades y participar en ejercicios de preparación.

La evolución reciente de la Unión Europea refuerza esta tendencia. La Directiva (UE) 2022/2557 derogó la Directiva 2008/114/CE y desplazó el énfasis desde la simple identificación de infraestructuras críticas hacia la resiliencia de entidades críticas. Esta transición es significativa para la República Dominicana: el objetivo ya no debe ser únicamente proteger instalaciones, sino asegurar la continuidad de servicios esenciales ante incidentes físicos, cibernéticos, naturales, tecnológicos o híbridos (Consejo de la Unión Europea, 2008; Parlamento Europeo y Consejo de la Unión Europea, 2022). La línea española más reciente también confirma el tránsito institucional hacia esquemas de protección y resiliencia de entidades públicas y privadas que operan en sectores estratégicos (Ministerio del Interior de España, 2026).

SITUACIÓN NORMATIVA DOMINICANA

La República Dominicana ha desarrollado instrumentos normativos relacionados con la gestión de riesgos, los delitos de alta tecnología, el terrorismo y la ciberseguridad. No obstante, estos instrumentos no conforman todavía un régimen integral de protección de infraestructuras críticas. El concepto aparece asociado principalmente a ciberseguridad o gestión de riesgos, sin una ley marco que establezca definiciones, catálogo, órgano rector, sectores estratégicos, responsabilidades de operadores, planes de seguridad y mecanismos de auditoría.

La Ley núm. 147-02 sobre Gestión de Riesgos constituye una base importante para la prevención, mitigación, preparación, respuesta y recuperación frente a desastres. Su enfoque interinstitucional y multidisciplinario es valioso para una política de infraestructuras críticas, especialmente frente a amenazas naturales, emergencias y desastres. Sin embargo, su propósito principal es la gestión del riesgo de desastres, no la identificación y protección permanente de infraestructuras críticas como categoría jurídica autónoma. (Ley No. 147-02, 2002).

La Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología aporta herramientas penales frente a delitos informáticos y conductas que afectan sistemas de información. Esta norma es relevante en la protección de sistemas digitales esenciales, pero tampoco equivale a un régimen integral de protección de infraestructuras críticas. Penalizar conductas cibernéticas es necesario, pero no sustituye la obligación de identificar operadores críticos, evaluar interdependencias, establecer planes de continuidad, fijar estándares de seguridad y coordinar respuestas ante incidentes. (Ley No. 53-07, 2007).

La Ley núm. 267-08 sobre Terrorismo incorpora una dimensión relevante frente a amenazas



deliberadas. La protección de infraestructuras críticas debe considerar terrorismo, sabotaje, crimen organizado y ataques híbridos. Sin embargo, la respuesta antiterrorista, por sí sola, no cubre la totalidad del problema, pues las infraestructuras críticas también pueden verse afectadas por fallas técnicas, errores humanos, fenómenos naturales, ciberataques, conflictos geopolíticos, pandemias, interrupciones logísticas y vulnerabilidades sistémicas. (Ley No. 267-08, 2008).

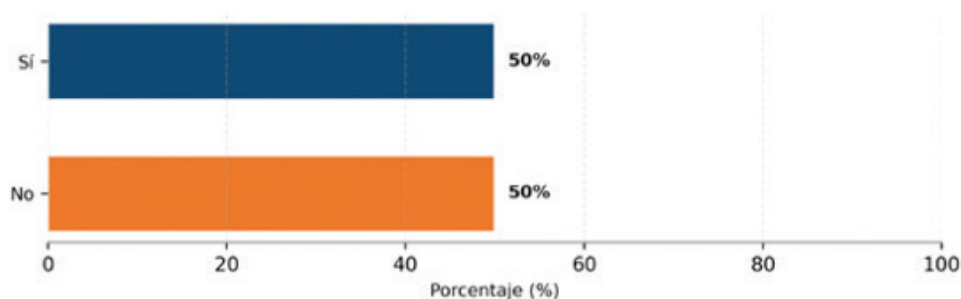
El avance más explícito se observa en la política nacional de ciberseguridad. El Decreto núm. 230-18 estableció la Estrategia Nacional de Ciberseguridad 2018-2021 y el Decreto núm. 313-22 aprobó la Estrategia Nacional de Ciberseguridad 2030. En el marco de esta última, el Centro Nacional de Ciberseguridad inició trabajos para un análisis nacional de riesgo orientado a identificar infraestructuras críti-

cas de información, con apoyo de programas internacionales. Este avance es significativo, pero mantiene un enfoque predominantemente cibernético. La República Dominicana necesita extender ese esfuerzo hacia un régimen integral que abarque infraestructura física, servicios esenciales, continuidad operativa, interoperabilidad institucional y resiliencia nacional. (Centro Nacional de Ciberseguridad, 2018, 2022; Ministerio de la Presidencia de la República Dominicana, 2022).

Por tanto, el problema dominicano no consiste en ausencia total de normas relacionadas, sino en dispersión normativa y falta de integración sistémica (ver figura 2). Existen piezas útiles, pero no una arquitectura legal que organice el sistema completo de protección y resiliencia de infraestructuras críticas.

Figura 2

Percepción sobre la existencia de legislación específica de protección de infraestructuras críticas en República Dominicana.



Nota: Elaboración propia con base en encuesta exploratoria aplicada por el autor el 27 de septiembre de 2021 a diez participantes vinculados a Fuerzas Armadas, CESAC, INDOTEL, IDAC, instituciones estatales y sector privado. Los resultados tienen alcance diagnóstico exploratorio y no valor estadístico representativo nacional.

BRECHA JURÍDICO-INSTITUCIONAL

La comparación entre España y la República Dominicana permite identificar una brecha jurídico-institucional concreta. España cuenta con definiciones específicas, órganos de coordinación, catálogo nacional, instrumentos de

planificación y obligaciones para operadores críticos. República Dominicana cuenta con normas sectoriales relevantes, pero carece de un sistema integral que articule esas piezas bajo una política nacional específica de infraestructuras críticas (ver cuadro 1).



Cuadro 1

Sectores de infraestructuras críticas en España y brechas observables en República Dominicana.

Sector en España	Tratamiento en España	Situación en República Dominicana	Brecha principal identificada
Energía	Sector crítico con planificación y coordinación específica	Protección dispersa entre normas sectoriales y gestión de riesgos	No existe clasificación integral ni plan nacional de protección
Agua	Servicio esencial incluido en el sistema de protección	Relevancia reconocida, pero sin régimen específico como infraestructura crítica	Falta identificación formal de activos y protocolos de continuidad
Transporte	Cobertura para redes aéreas, marítimas y terrestres	Alta relevancia logística y turística, sin esquema integral de protección crítica	Ausencia de catálogo Nacional y planes por operador
TIC	Sector crítico articulado con ciberseguridad y resiliencia	Avances en ciberseguridad, pero sin integración plena con infraestructura crítica	Enfoque parcial centrado en ciberseguridad y no en continuidad multisectorial
Salud	Servicios esenciales contemplados para continuidad operativa	Importancia estratégica evidente tras la pandemia	No hay marco de protección crítica para hospitales, laboratorios y cadenas asociadas
Sistema financiero y tributario	Sector definido por su impacto sistémico	Importancia institucional clara, pero sin clasificación como infraestructura crítica	Falta un esquema legal que articule resiliencia, supervisión y respuesta coordinada
Alimentación	Protección de cadenas de abastecimiento esenciales	Dependencia de importaciones y logística de distribución	No existe diseño normativo específico para continuidad del abastecimiento crítico
Administración pública	Funciones esenciales incluidas en la continuidad del Estado	Capacidades institucionales dispersas	Ausencia de órgano rector especializado e instrumentos de coordinación público-privada

Nota: Elaboración propia con base en la Ley 8/2011, el Real Decreto 704/2011 y el análisis comparado desarrollado por el autor.

IMPLICACIONES PARA LA SEGURIDAD Y DEFENSA NACIONAL

La protección de infraestructuras críticas tiene una relación directa con la seguridad y defensa nacional. En un Estado moderno, la defensa no se limita a la protección territorial frente a amenazas militares tradicionales; también comprende la preservación de capacidades esenciales para sostener la vida nacional durante crisis, emergencias, ataques deliberados o interrupciones sistémicas. Desde esta perspectiva, la seguridad energética, hídrica, aeroportuaria, portuaria, financiera, sanitaria y digital debe ser comprendida como parte del ecosistema estratégico de la nación.

La República Dominicana posee características que intensifican esa relación. Su condición insu-

lar, su dependencia de puertos y aeropuertos para comercio, turismo y movilidad internacional, su exposición a huracanes y fenómenos hidrometeorológicos, la concentración de servicios en zonas urbanas y la creciente digitalización de procesos públicos y privados convierten la continuidad de servicios esenciales en un asunto de seguridad nacional. Una interrupción prolongada en energía, telecomunicaciones, transporte aéreo, abastecimiento de agua o sistemas financieros tendría impactos superiores al daño sectorial inmediato.

La defensa nacional también debe considerar amenazas híbridas. Un actor hostil no necesita atacar directamente una instalación militar para afectar la seguridad del Estado. Puede intentar perturbar servicios logísticos, comunicaciones, sistemas de navegación, redes eléctricas,



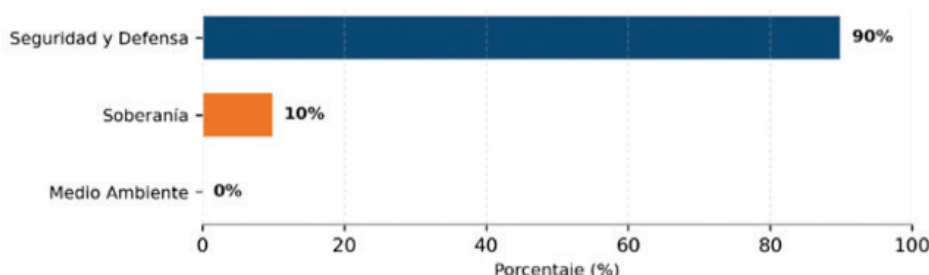
plataformas digitales, cadenas de suministro o infraestructuras aeroportuarias. De ahí que la protección de infraestructuras críticas deba integrarse con la planificación de defensa, inteli-

gencia, ciberdefensa, seguridad aeroportuaria, protección marítima, gestión de emergencias y continuidad gubernamental.

Figura 3

Pertinencia del tema para la seguridad y defensa nacional.

Nota: Elaboración propia con base en encuesta exploratoria aplicada por el autor el 27 de septiembre de 2021 a diez participantes vinculados a Fuerzas Armadas, CESAC, INDOTEL, IDAC, instituciones estatales y sector privado.



Los resultados tienen alcance diagnóstico exploratorio y no valor estadístico representativo nacional.

SECTORES ESTRATÉGICOS PRIORITARIOS PARA LA REPÚBLICA DOMINICANA

Una política nacional de infraestructuras críticas debe priorizar sectores según impacto y realidad nacional. Para la República Dominicana, el sector energético es central, porque sostiene servicios públicos, actividades económicas, salud, educación, transporte, seguridad y comunicaciones. Cualquier interrupción significativa de generación, transmisión o distribución eléctrica puede producir efectos en cascada sobre otros sectores.

El sector agua debe ocupar un lugar prioritario. Plantas de tratamiento, sistemas de distribución, presas, acueductos, estaciones de bombeo y redes de saneamiento son esenciales para salud pública, actividad económica y estabilidad social. La experiencia internacional demuestra que agua potable y saneamiento son servicios cuya interrupción puede convertirse rápidamente en crisis humanitaria, sanitaria y de orden público.

El transporte aéreo y marítimo reviste importancia estratégica. Aeropuertos internacionales, puertos, terminales logísticas, sistemas de navegación, radares, control del espacio aéreo, almacenamiento de combustibles y cadenas de suministro son nodos críticos para comercio, turismo, ayuda humanitaria, evacuaciones, defensa, seguridad fronteriza y conectividad internacional. En un país con fuerte dependencia turística y comercial, la resiliencia de estos nodos debe ser prioritaria.

El sector telecomunicaciones y tecnologías de la información constituye una infraestructura transversal. Redes móviles, fibra óptica, centros de datos, plataformas gubernamentales, servicios bancarios digitales, sistemas de emergencia y redes de comunicación institucional sostienen la capacidad de respuesta del Estado y la continuidad de actividades privadas. Su protección debe integrarse con ciberseguridad, continuidad operativa y redundancia técnica.



El sistema financiero, la salud, la alimentación, la administración pública, la seguridad y la defensa también requieren análisis sectorial. La designación de sectores críticos no implica militarizar su gestión, sino reconocer que su interrupción puede afectar funciones vitales de la sociedad. La clasificación debe permitir priorizar recursos, definir obligaciones, proteger información sensible y establecer mecanismos de coordinación.

DISCUSIÓN COMPARADA:
ADAPTACIÓN DEL MODELO
ESPAÑOL

La adopción de un modelo dominicano no debe entenderse como simple trasplante normativo. España opera dentro de un marco europeo, con obligaciones derivadas de directivas comunitarias, una arquitectura administrativa distinta y capacidades institucionales acumuladas. La República Dominicana debe aprovechar la experiencia comparada, pero construir una solución coherente con su Constitución, su organización administrativa, su sistema de seguridad y defensa, su régimen de gestión de riesgos y su estructura económica.

En América Latina se observan niveles desiguales de madurez frente al modelo español. Brasil presenta uno de los avances más cercanos al contar con una política, una estrategia y un plan nacional de seguridad de infraestructuras críticas; Chile avanza mediante una ley marco de ciberseguridad e infraestructura crítica de la información que crea una autoridad especializada y obligaciones para entidades públicas y privadas que prestan servicios esenciales; Colombia desarrolla lineamientos de gobernanza de seguridad digital, identificación de infraestructuras críticas cibernéticas y servicios esenciales; y Argentina cuenta con definiciones, criterios de identificación y sectores alcanzados dentro de su política de infraestructuras críticas de información. Estos casos se aproximan parcialmente al modelo español, pero en general mantienen mayor énfasis digital o sectorial y menor desarrollo integral de catálogo reservado, planificación escalonada y obligaciones físico-cibernéticas equivalentes a las previstas en España (República Argentina, 2019; República de Chile, 2024; República de Colombia, 2022; República Federativa del Brasil, 2022).

Cuadro 2
Experiencias latinoamericanas de protección de infraestructuras críticas
y comparación con el modelo español.

País	Instrumento principal	Alcance del modelo	Nivel respecto al modelo español
Brasil	Política, Estrategia Nacional y Plan Nacional de Seguridad de Infraestructuras Críticas.	Incluye organización estatal, sectores estratégicos y medidas de protección coordinadas.	Nivel alto de aproximación regional: más cercano a España en planificación nacional, aunque con estructura propia.
Chile	Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información, Ley No. 21.663.	Crea autoridad nacional y obligaciones para entidades públicas y privadas que prestan servicios esenciales.	Nivel medio-alto: avance sólido, pero centrado principalmente en infraestructura crítica de información.
Colombia	Decreto No. 338 de 2022 sobre gobernanza de seguridad digital.	Define infraestructura crítica cibernética, servicios esenciales, gestión de riesgos y respuesta a incidentes.	Nivel medio: relevante para ciberseguridad y servicios esenciales, pero no equivalente a un sistema integral físico-cibernético.
Argentina	Resolución 1523/2019 y normas complementarias de ciberseguridad.	Aprueba definiciones, criterios de identificación y sectores vinculados a infraestructuras críticas e infraestructuras críticas de información.	Nivel medio: útil como referencia conceptual, aunque con menor desarrollo operativo que el modelo español.

Nota: Elaboración propia con base en República Argentina (2019), República de Chile (2024), República de Colombia (2022) y República Federativa del Brasil (2022).



El principal valor del modelo español no está en copiar sus órganos, sino en comprender su lógica: identificación de sectores, catálogo reservado, planificación escalonada, obligaciones de operadores, coordinación pública y privada, niveles de alerta, planes de apoyo operativo y autoridad nacional competente. Estos componentes pueden adaptarse al contexto dominicano mediante una arquitectura más flexible, gradual y proporcional, que permita empezar por sectores prioritarios y ampliar el sistema conforme aumenten las capacidades institucionales.

Una estrategia prudente sería aplicar un modelo por fases. La primera fase consistiría en aprobar definiciones, autoridad coordinadora y metodología nacional de criticidad. La segunda fase debería identificar sectores prioritarios y elaborar un catálogo inicial reservado. La tercera fase podría exigir planes de seguridad y continuidad a operadores críticos seleccionados. La cuarta fase integraría ejercicios interinstitucionales, auditorías y cooperación internacional. Este enfoque reduce resistencia institucional y evita crear obligaciones imposibles de cumplir en el corto plazo.

La adaptación dominicana también debe reconocer el papel de las Fuerzas Armadas. Su función no sería sustituir a reguladores sectoriales ni administrar infraestructuras privadas, sino apoyar la planificación estratégica, la protección de instalaciones esenciales cuando proceda, la defensa del espacio aéreo y marítimo, la respuesta ante crisis, la ciberdefensa, la logística, la inteligencia y la cooperación internacional. La protección de infraestructuras críticas es una misión de Estado, no de una sola institución.

PROPUESTA ESTRATÉGICA PARA LA REPÚBLICA DOMINICANA

La República Dominicana debería avanzar hacia una Ley Marco de Protección y Resiliencia de Infraestructuras Críticas. Esta ley debe es-

tablecer principios, definiciones, órganos competentes, sectores estratégicos, obligaciones de operadores, instrumentos de planificación, criterios de clasificación, mecanismos de coordinación y régimen de confidencialidad de la información crítica. El objetivo no debe ser replicar mecánicamente el modelo español, sino adaptarlo a la realidad geográfica, institucional, económica y de seguridad nacional dominicana.

El primer componente debe ser un Sistema Nacional de Protección y Resiliencia de Infraestructuras Críticas. Este sistema integraría a las instituciones responsables de seguridad, defensa, gestión de riesgos, ciberseguridad, protección civil, regulación sectorial, inteligencia, transporte, energía, agua, salud, finanzas, telecomunicaciones y sector privado. Su función sería coordinar políticas, aprobar planes, establecer niveles de alerta, supervisar ejercicios y definir criterios técnicos de protección.

El segundo componente debe ser un órgano coordinador nacional. Puede crearse un Centro Nacional de Protección y Resiliencia de Infraestructuras Críticas o una unidad especializada adscrita a una autoridad de alto nivel. Su función sería elaborar y custodiar el catálogo nacional, coordinar con operadores críticos, emitir lineamientos técnicos, integrar información de riesgos, articular con el Centro Nacional de Ciberseguridad y apoyar la toma de decisiones estratégicas.

El tercer componente debe ser el Catálogo Nacional de Infraestructuras Estratégicas y Críticas. Este instrumento debe contener información clasificada sobre instalaciones, redes, sistemas, operadores, ubicación, titularidad, servicios prestados, interdependencias, nivel de criticidad, amenazas, vulnerabilidades, capacidades de respuesta y planes asociados. Por razones de seguridad nacional, el catálogo debe ser reservado, actualizado y administrado bajo protocolos estrictos.



El cuarto componente debe ser la sectorización. En una primera etapa, la República Dominicana podría priorizar los sectores de energía, agua, salud, transporte aéreo y marítimo, telecomunicaciones, sistemas financieros, alimentación, administración pública, seguridad, defensa y tecnologías de la información. La priorización debe considerar impacto social, impacto económico, número de usuarios afectados, tiempo de recuperación, ausencia de alternativas, impacto transfronterizo e incidencia en el orden público.

El quinto componente debe ser el sistema de planes. Se recomienda establecer un Plan Nacional de Protección y Resiliencia de Infraestructuras Críticas, planes estratégicos sectoriales, planes de seguridad del operador, planes de protección específicos y planes de apoyo operativo. Estos instrumentos deben definir medidas preventivas, responsables, protocolos de comunicación, niveles de alerta, procedimientos de respuesta, rutas de recuperación y mecanismos de evaluación periódica.

El sexto componente debe ser la obligación de los operadores críticos. Todo operador designado debería elaborar análisis de riesgo, plan de seguridad, plan de continuidad, plan de respuesta a incidentes, protocolo de comunicación

con autoridades, designación de un responsable de seguridad y participación en ejercicios. La ley debe prever obligaciones proporcionales, protección de información sensible y mecanismos de supervisión.

El séptimo componente debe ser la articulación ciber-física. La Estrategia Nacional de Ciberseguridad 2030 puede servir como plataforma inicial para infraestructuras críticas de información, pero debe integrarse con una visión más amplia. La convergencia entre sistemas físicos, tecnologías operacionales, redes digitales, sensores, telecomunicaciones y plataformas de gestión obliga a tratar ciberseguridad, seguridad física y continuidad operativa como dimensiones complementarias.

El octavo componente debe ser la formación y cultura de seguridad. La protección de infraestructuras críticas no será efectiva si se limita a documentos. Debe traducirse en doctrina, capacitación, ejercicios interinstitucionales, simulaciones, auditorías, protocolos de intercambio de información y cultura de resiliencia. La Universidad Nacional para la Defensa, las academias militares, las instituciones de gestión de riesgos y los centros especializados podrían desempeñar un papel central en la formación de cuadros técnicos y estratégicos.

CONCLUSIONES

La protección de infraestructuras críticas debe ser entendida como una función estratégica del Estado. En República Dominicana, los avances en ciberseguridad, gestión de riesgos y persecución de delitos de alta tecnología constituyen bases importantes, pero no sustituyen la necesidad de una ley marco específica que organice un sistema nacional integral.

El modelo español demuestra que la protección de infraestructuras críticas requiere definiciones legales, órganos responsables, catálogo

nacional, planes de actuación, obligaciones de operadores y coordinación público-privada. Su evolución reciente hacia la resiliencia de entidades críticas confirma que el enfoque contemporáneo no se limita a proteger activos, sino a asegurar la continuidad de servicios esenciales.

La República Dominicana posee condiciones que hacen urgente esta discusión: insularidad, dependencia de nodos logísticos, portuarios y aeroportuarios, alta relevancia del turismo, concentración urbana, exposición a fenómenos



naturales, crecimiento digital, dependencia de telecomunicaciones, interconexión energética y riesgos derivados del crimen organizado, ciberataques y amenazas híbridas.

El país necesita avanzar hacia un Sistema Nacional de Protección y Resiliencia de Infraestructuras Críticas que integre seguridad nacional, defensa, ciberseguridad, gestión de riesgos, continuidad operativa y cooperación público-privada. La creación de una ley marco, un órgano coordinador, un catálogo nacional y planes sectoriales permitirá fortalecer la seguridad nacional, proteger servicios esenciales y aumentar la resiliencia institucional ante crisis futuras.

Como limitaciones del estudio, debe precisarse que la comparación jurídica se concentra en España como modelo principal, con referencias latinoamericanas complementarias, y que la encuesta utilizada tiene alcance exploratorio por su tamaño y modalidad de selección. En consecuencia, los resultados gráficos no deben interpretarse como medición nacional de percepción institucional, sino como apoyo diagnóstico pre-

liminar para contextualizar la necesidad de mayor desarrollo normativo e institucional.

Como futuras líneas de investigación, se recomienda desarrollar estudios sectoriales sobre energía, agua, transporte aéreo y marítimo, telecomunicaciones, salud, finanzas y alimentación; diseñar una metodología nacional de criticidad; comparar experiencias de otros Estados insulares y caribeños; y validar, mediante entrevistas a expertos y ejercicios de simulación, un modelo dominicano de coordinación público-privada para la continuidad de servicios esenciales.

En síntesis, la pregunta no es si la República Dominicana debe legislar sobre infraestructuras críticas, sino cuándo y con qué nivel de ambición estratégica. La experiencia comparada demuestra que los Estados que identifican, protegen y hacen resilientes sus servicios esenciales están mejor preparados para enfrentar amenazas complejas, preservar la estabilidad y garantizar la continuidad de las funciones vitales de la nación.

REFERENCIAS

- Ampratwum, G., Osei-Kyei, R., & Tam, V. W. Y. (2022). Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events: A systematic review. *International Journal of Critical Infrastructure Protection*, 39, 100556. <https://doi.org/10.1016/j.ijcip.2022.100556>
- Baralt Blanco, N. (2021). Infraestructuras críticas y ciberseguridad en las fuerzas armadas dominicanas. *Revista Seguridad, Ciencia & Defensa*, 5(5), 13-21. <https://doi.org/10.59794/rscd.2019.v5i5.57>
- Centro Nacional de Ciberseguridad. (2018). Decreto No. 230-18. Que establece y regu-
- la la Estrategia Nacional de Ciberseguridad 2018-2021. *Gaceta Oficial*. Santo Domingo, República Dominicana. 2 de julio de 2018, núm. 10912. <https://cncs.gob.do/wp-content/uploads/2020/02/Decreto-230-18.pdf>
- Centro Nacional de Ciberseguridad. (2022). Decreto No. 313-22. Que aprueba la Estrategia Nacional de Ciberseguridad 2030. *Gaceta Oficial*. Santo Domingo, República Dominicana. 14 de junio de 2022, núm. 11068. <https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf>
- Centro Nacional de Ciberseguridad. (2024). Plan de acción 2022-2024 de la Estrategia Nacional de Ciberseguridad 2030. <https://>



- cncs.gob.do/wp-content/uploads/2024/06/Plan-de-Accion-2022-2024-ENCS-2030.pdf
- Consejo de la Unión Europea. (2008). Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Diario Oficial de la Unión Europea, L 345, 75-82. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32008L0114>
- Ley No. 147-02. Sobre Gestión de Riesgos. Gaceta Oficial. Santo Domingo, República Dominicana. 22 de septiembre de 2002, núm. 10172. https://gobiernodesantodomingo.gob.do/wp-content/uploads/2024/07/Ley_147_02_sobre_gestion_de_riesgos.pdf
- Ley No. 53-07. Sobre Crímenes y Delitos de Alta Tecnología. Gaceta Oficial. Santo Domingo, República Dominicana. 9 de mayo de 2007, núm. 10416. https://mip.gob.do/transparencia/images/docs/base_legal/Ley_53-07.pdf
- Ley No. 267-08. Sobre Terrorismo, y que crea el Comité Nacional Antiterrorista y la Dirección Nacional Antiterrorista. Gaceta Oficial. Santo Domingo, República Dominicana. 4 de julio de 2008, núm. 10476. <https://www.dgii.gov.do/legislacion/leyesTributarias/Documents/Otras%20Leyes%20de%20Inter%C3%A9s/267-08.pdf>
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Boletín Oficial del Estado. Madrid, España. 29 de abril de 2011, núm. 102, pp. 43370-43380. <https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630>
- Ministerio de la Presidencia de la República Dominicana. (2022, 20 de julio). Ciberseguridad trabaja en identificar infraestructuras críticas de la información. <https://minpre.gob.do/comunicacion/notas-de-prensa/ciberseguridad-trabaja-en-identificar-infraestructuras-criticas-de-la-informacion/>
- Ministerio del Interior de España. (2026, 17 de marzo). El Gobierno aprueba una ley de protección y resiliencia de las entidades públicas y privadas que operan en los sectores estratégicos. <https://www.interior.gob.es/opencms/es/detalle/articulo/El-Gobierno-aprueba-una-ley-de-proteccion-y-resiliencia-de-las-entidades-publicas-y-privadas-que-operan-en-los-sectores-estrategicos/>
- Osei-Kyei, R., Almeida, L. M., Ampratwum, G., & Tam, V. W. Y. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation*, 23(5), 1210-1231. <https://doi.org/10.1108/CI-03-2021-0047>
- Parlamento Europeo y Consejo de la Unión Europea. (2022). Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE. Diario Oficial de la Unión Europea, L 333, 164-198. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
- Rathnayaka, B., Siriwardana, C. S. A., Robert, D., Amaratunga, D., & Setunge, S. (2022). Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. *International Journal of Disaster Risk Reduction*, 78, Article 103123. <https://doi.org/10.1016/j.ijdr.2022.103123>
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Boletín Oficial del Estado. Madrid, España. 21 de mayo de 2011, núm. 121, pp. 50808-50826. <https://www.boe.es/buscar/act.php?id=BOE-A-2011-8849>



- República Argentina. (2019). Resolución 1523/2019. Apruébase la definición de infraestructuras críticas y de infraestructuras críticas de información, criterios de identificación y sectores alcanzados. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 13 de septiembre de 2019. <https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1523-2019-328599>
- República de Chile. (2024). Ley No. 21.663. Ley marco de ciberseguridad. Diario Oficial de la República de Chile. Santiago de Chile. 8 de abril de 2024. <https://www.bcn.cl/ley-chile/navegar?idNorma=1202434>
- República de Colombia. (2022). Decreto No. 338 de 2022. Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, con el fin de establecer 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. Diario Oficial. Bogotá, Colombia. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>
- República Federativa del Brasil. (2022). Decreto No. 11.200, de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União. Brasília, Brasil. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11200.htm
- Vidal López, R. (2017, 22 de abril). El sistema PIC. Un centauro en el desierto. <https://uncentauroeneldesierto.com/2017/04/22/el-sistema-pic/>
- Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*, 15, Article 100244. <https://doi.org/10.1016/j.pdisas.2022.100244>
- Yang, Z., Barroca, B., Weppe, A., Bony-Dandrieux, A., Laffréchine, K., Daclin, N., November, V., Omrane, K., Kamissoko, D., Benaben, F., Dolidon, H., Tixier, J., & Chapurlat, V. (2023). Indicator-based resilience assessment for critical infrastructures: A review. *Safety Science*, 160, 106049. <https://doi.org/10.1016/j.ssci.2022.106049>
- Yang, Z., Barroca, B., Mebarki, A., Laffréchine, K., Dolidon, H., & Lilas, L. (2024). Critical infrastructure resilience: A guide for building indicator systems based on a multi-criteria framework with a focus on implementable actions. *Natural Hazards and Earth System Sciences*, 24, 3723-3753. <https://doi.org/10.5194/nhess-24-3723-2024>
- Yu, D. J., Shin, H. C., Olivier, T., Garcia, M., Meerow, S., & Park, J. (2025). Logical interdependencies in infrastructure: What are they, how to identify them, and what do they mean for infrastructure risk analysis? *Risk Analysis*, 45, 356-375. <https://doi.org/10.1111/risa.16555>

