EXPOSICIÓN DE MOTIVOS

ANTEPROYECTO DE LEY DE INFRAESTRUCTURAS CRÍTICAS Y SERVICIOS ESENCIALES.

La República de Panamá ocupa una posición geopolítica singular en el sistema internacional. Su ubicación estratégica como punto de conexión interoceánica, la operación del Canal de Panamá, su plataforma logística multimodal, su centro bancario internacional, sus puertos, aeropuertos, zonas francas, infraestructura energética y redes de telecomunicaciones, la convierten en un nodo esencial del comercio global y en un actor clave para la estabilidad económica regional y hemisférica.

Esta condición estratégica, que constituye una fortaleza estructural para el desarrollo nacional, también implica una exposición elevada a riesgos geopolíticos, económicos, híbridos y cibernéticos, derivados de tensiones internacionales, competencia entre potencias, conflictos transnacionales, criminalidad organizada y actores estatales o no estatales con capacidades avanzadas.

En el contexto contemporáneo, las infraestructuras críticas y los servicios esenciales han dejado de ser meros activos económicos para convertirse en objetivos estratégicos en escenarios de rivalidad geopolítica. Las tendencias globales demuestran que la afectación deliberada de sistemas energéticos, redes eléctricas, telecomunicaciones, puertos, sistemas financieros o infraestructuras de transporte puede utilizarse como instrumento de presión económica, desestabilización institucional o interferencia estratégica.

El ciberespacio se ha consolidado como un dominio operativo adicional, junto a los dominios terrestre, marítimo, aéreo y espacial, en el cual se desarrollan actividades de espionaje, sabotaje, influencia indebida y operaciones híbridas. Los ataques cibernéticos dirigidos contra infraestructuras críticas ya no son hipótesis teóricas, sino realidades documentadas en múltiples jurisdicciones, con impactos económicos multimillonarios y efectos sistémicos prolongados.

Panamá, como plataforma global de tránsito y servicios, no está aislada de estas dinámicas. Por el contrario, su relevancia estratégica incrementa su perfil de riesgo. La interdependencia digital, la tercerización tecnológica, la dependencia de proveedores internacionales, la integración en cadenas globales de suministro y la presencia de inversiones extranjeras en sectores estratégicos hacen indispensable un marco normativo integral que articule seguridad, gobernanza, cumplimiento e interés nacional.

La protección de las infraestructuras críticas y los servicios esenciales debe entenderse, por tanto, como una política de Estado vinculada directamente a la seguridad nacional, a la continuidad del Estado y a la preservación de la soberanía funcional.

La ausencia de una legislación específica y coherente en materia de protección integral de infraestructuras críticas genera dispersión normativa, fragmentación institucional, y vacíos en la asignación de responsabilidades. En un entorno de riesgos sistémicos y amenazas híbridas, dicha fragmentación debilita la capacidad preventiva del Estado y limita la eficacia de la respuesta ante incidentes de alto impacto.

El presente Anteproyecto establece un marco jurídico moderno que define claramente las competencias institucionales, que establece obligaciones proporcionales al nivel de riesgo y criticidad, que integra seguridad física y cibernética bajo un enfoque unificado, que incorpora mecanismos de cumplimiento

normativo y debida diligencia, fortaleciendo la coordinación interinstitucional y la cooperación público-privada, e integrando la supervisión, fiscalización y potestad sancionadora bajo criterios técnicos.

Este modelo responde a estándares internacionales emergentes en materia de protección de infraestructuras críticas y resiliencia nacional, adaptados a la realidad panameña.

En el actual entorno internacional, los riesgos no se limitan a ataques directos. Existen formas indirectas de vulnerabilidad que pueden comprometer sectores estratégicos, tales como estructuras societarias opacas, falta de identificación de beneficiarios finales, la influencia significativa de actores extranjeros en activos estratégicos, la dependencia tecnológica excesiva de proveedores específicos, la vulnerabilidades en la cadena de suministro, y la captura regulatoria o corrupción.

El Anteproyecto reconoce que la inversión extranjera es un motor legítimo del desarrollo nacional. Sin embargo, en sectores críticos, el análisis de riesgos estratégicos asociados a propiedad, control o influencia extranjera debe realizarse mediante criterios técnicos, objetivos y proporcionales, orientados exclusivamente a la protección del interés nacional.

Este enfoque se fundamenta en el principio de neutralidad y no discriminación: la evaluación se realizará con base en gestión de riesgos estratégicos, no en consideraciones arbitrarias de nacionalidad, respetando los tratados internacionales y el régimen de inversión vigente en Panamá.

Asimismo, se incorpora la obligación de identificar y verificar beneficiarios finales de operadores críticos y proveedores relevantes, como mecanismo de transparencia estructural que fortalece la seguridad nacional y previene riesgos de infiltración o interferencia indebida.

La seguridad de infraestructuras críticas no puede depender exclusivamente de controles tecnológicos. Requiere estructuras organizacionales sólidas y cultura de cumplimiento.

Por ello, el Anteproyecto introduce el principio de cumplimiento normativo como eje transversal, exigiendo a los operadores críticos y a los actores de la cadena de suministro, con programas internos de cumplimiento, evaluaciones periódicas de riesgos físicos, cibernéticos y estratégicos, procedimientos de debida diligencia en contratación de terceros, políticas de integridad y prevención de conflictos de interés, sistemas de control interno y auditoría, y programas antisoborno y anticorrupción.

La corrupción constituye un vector de riesgo estratégico, pues puede facilitar accesos indebidos, debilitamiento de controles y vulneración deliberada de estándares de seguridad. La implementación de programas antisoborno no solo responde a compromisos internacionales de Panamá, sino que fortalece la resiliencia estructural de sectores críticos.

El fortalecimiento de la seguridad nacional debe desarrollarse dentro del marco del Estado de Derecho. El Anteproyecto reafirma que toda actuación de la autoridad competente deberá fundarse en la Constitución y la ley, respetar el debido proceso, aplicar criterios de proporcionalidad y razonabilidad técnica, garantizar la confidencialidad de información sensible, y proteger los derechos fundamentales.

La protección de infraestructuras críticas no es incompatible con la transparencia y la rendición de cuentas. Por el contrario, la legitimidad del sistema descansa en el equilibrio entre seguridad y respeto a los derechos humanos.

La arquitectura institucional propuesta se basa en un modelo de gobernanza diferenciada, con dirección estratégica de alto nivel, fiscalización técnica permanente, y potestad sancionadora especializada.

Este esquema fortalece la coherencia institucional, evita duplicidades y permite respuestas ágiles ante incidentes complejos.

La fiscalización se concibe como técnica, preventiva y basada en gestión de riesgos, no como intervención arbitraria. Se busca verificar cumplimiento, reducir vulnerabilidades y promover mejora continua.

Las amenazas a infraestructuras críticas son transnacionales por naturaleza. Por ello, la Ley promueve la cooperación público-privada, el intercambio seguro de información, la vinculación con la academia y centros de investigación, la coordinación con sociedad civil especializada, la cooperación con países aliados, la participación en redes internacionales de protección de infraestructuras críticas y Ciberseguridad, y la integración en redes globales fortalece capacidades técnicas, anticipación estratégica y respuesta coordinada ante incidentes de alcance internacional.

El Anteproyecto adopta un enfoque preventivo y de gestión integral del riesgo. La resiliencia se define como la capacidad de continuar operando incluso bajo ataque, adaptarse a condiciones adversas y recuperar servicios esenciales en el menor tiempo posible.

La seguridad ya no puede basarse únicamente en la protección perimetral debe integrar la prevención, la detección temprana, la respuesta coordinada, la recuperación estructurada, y la mejora continua.

La presente iniciativa legislativa constituye una herramienta estratégica para consolidar la soberanía funcional, la estabilidad institucional y la competitividad internacional de Panamá.

En un entorno geopolítico caracterizado por rivalidades estratégicas, amenazas híbridas y creciente instrumentalización de infraestructuras críticas como objetivos de presión económica o política, el Estado panameño requiere un marco jurídico robusto, coherente y prospectivo que garantice la protección, seguridad y resiliencia de sus activos más sensibles.

Este Anteproyecto no representa una medida aislada, sino una política de Estado orientada a preservar la continuidad del país, la confianza internacional, la inversión responsable y la seguridad de las generaciones presentes y futuras.

Por las razones expuestas, se somete a consideración de la Asamblea Nacional el presente Anteproyecto de Ley como instrumento esencial para fortalecer la seguridad estratégica y la resiliencia nacional de la República de Panamá en el siglo XXI.

Anteproyecto de Ley No. ____

(De __ de _____ de 2026).

"Ley de Infraestructuras Críticas y Servicios Esenciales".

LA ASAMBLEA NACIONAL

DECRETA:

Capítulo I
Disposiciones Generales.

Artículo 1. Objeto: La presente Ley tiene por objeto establecer el marco jurídico, estratégico y operativo para seguridad, protección y resiliencia de las Infraestructuras Críticas y los Servicios Esenciales en la República de Panamá, mediante la creación de mecanismos, competencias y obligaciones que permitan prevenir, identificar, detectar, responder y recuperar ante riesgos, amenazas o incidentes físicos o cibernéticos, que tengan un efecto debilitante en la economía nacional, el bienestar de la población, la seguridad nacional o la continuidad del Estado.

Artículo 2. Ámbito de Aplicación: La presente Ley se aplica y establece obligaciones a todos los operadores críticos públicos y privados, que operen, gestionen o soporten o infraestructuras críticas o servicios esenciales en la República de Panamá, incluyendo sus datos, sistemas, instalaciones, redes, y plataformas digitales, en lo relativo a su seguridad, protección y continuidad operativa.

Quedan igualmente incluidos en el ámbito de aplicación de la presente Ley, los sectores críticos establecidos, las autoridades competentes, autoridades reguladoras sectoriales, autoridades rectoras, proveedores, contratistas y subcontratistas, cuyas competencias, actividades o servicios pudieran comprometer la seguridad, protección, resiliencia y/o la continuidad operativa de las infraestructuras críticas y los servicios esenciales.

Artículo 3. Principios Rectores: Para los efectos de esta Ley los principios rectores que guiarán su interpretación, aplicación y las acciones de protección y seguridad:

1. Principio de Cooperación: Este principio establece para que las autoridades, la sociedad civil, el sector académico, países aliados, y los actores vinculados a infraestructuras críticas y servicios esenciales deberán coordinar, colaborar e intercambiar información, a nivel nacional e internacional, de forma oportuna y proporcional, para prevenir y gestionar riesgos y amenazas físicas y cibernéticas, fortaleciendo la seguridad y resiliencia del Estado;
2. Principio de Coordinación: Este principio se establece para que las autoridades, reguladores sectoriales, operadores críticos, proveedores, contratistas y subcontratistas actúen de manera conjunta, sincronizada y armonizada, compartiendo información relevante y alineando procedimientos para asegurar una protección y respuesta eficaz frente a incidentes y amenazas de cualquier tipo;

3. Principio de Continuidad: Este principio se establece para que las autoridades, reguladores sectoriales, operadores críticos, proveedores, contratistas y subcontratistas, garanticen que los datos, sistemas, instalaciones, redes, activos y plataformas digitales permanezcan operativas incluso bajo ataque, asegurando la recuperación rápida y la mínima interrupción posible;
4. Principio de Integridad: Este principio se establece para que las autoridades, reguladores sectoriales, operadores críticos, proveedores, contratistas y subcontratistas, garanticen que los datos, sistemas, redes y plataformas digitales no sean alteradas, manipuladas, ni destruidos por actores maliciosos, o no maliciosos, fallas técnicas o accesos no autorizados;
5. Principio de Prevención: Este principio se establece para que las autoridades, reguladores sectoriales, operadores críticos, proveedores, contratistas y subcontratistas se anticipen a las amenazas, identificando vulnerabilidades y adoptando medidas técnicas, operativas y legales que reduzcan los riesgos antes de que ocurran;
6. Principio de Proporcionalidad: Este principio se establece para que las medidas de protección, respuesta, mitigación y sanciones, sean aplicadas de manera adecuada, necesaria, equilibrada y proporcional con la gravedad de la amenaza o incidente, evitando acciones excesivas o insuficientes;
7. Principio de Seguridad Nacional: Este principio establece que la protección y seguridad de las infraestructuras críticas y los servicios esenciales constituye un asunto de seguridad nacional.
   La interpretación y aplicación de la presente Ley deberá orientarse a garantizar la continuidad del Estado, la estabilidad institucional, la economía nacional y el bienestar de la población frente a amenazas o riesgos que puedan afectar su funcionamiento;
8. Principio de Fiscalización: Este principio se establece para que la protección de las infraestructuras críticas y servicios esenciales estará sujeta a supervisión técnica, permanente y proporcional de la autoridad competente, orientada a la prevención de riesgos y verificación del cumplimiento normativo, con respeto al debido proceso, la confidencialidad y la continuidad operativa;
9. Principio de Cumplimiento y Debida Diligencia: Este principio establece que establezca que los operadores críticos deben implementar sistemas internos para asegurar el cumplimiento permanente de la ley y de los estándares de seguridad física y cibernética;
10. Principio de Transparencia y Respeto a los Derechos Fundamentales: Se establece para que las medidas de protección de infraestructuras críticas y servicios esenciales se adoptarán con transparencia y rendición de cuentas, en armonía con la seguridad nacional y la reserva de información sensible, garantizando la legalidad, el debido proceso, la proporcionalidad y el respeto a los derechos fundamentales;
11. Principio de Legalidad: Se establece para que las actuaciones y medidas en materia de protección de infraestructuras críticas y servicios esenciales deberán fundarse en la Constitución y la ley, ejercerse dentro de las competencias atribuidas y ajustarse a los principios de seguridad jurídica y control, quedando prohibida toda actuación arbitraria;
12. Principio de Neutralidad y No Discriminación: Este principio se establece para que la evaluación de la propiedad, control o influencia extranjera sobre infraestructuras críticas y servicios esenciales se realizará con base en criterios técnicos, objetivos y proporcionales de riesgo estratégico, sin discriminación por razón de nacionalidad, y en plena observancia de la Constitución Política y los tratados internacionales suscritos por la República de Panamá.

13. Principio de Derechos Humanos: Este principio se establece para que la planificación, adopción y ejecución de políticas, medidas y actuaciones relativas a la protección de las infraestructuras críticas y los servicios esenciales deberán respetar, proteger y garantizar los derechos humanos y las libertades fundamentales reconocidos en la Constitución, los tratados internacionales ratificados por la República de Panamá y el ordenamiento jurídico vigente;
14. Principio de Integridad y Antisoborno: Se establece para que las actuaciones de los operadores críticos, proveedores, contratistas, subcontratistas, y las autoridades y reguladores sectoriales competentes deberán regirse por estándares de integridad, transparencia y prevención del soborno y la corrupción, implementando controles destinados a evitar que prácticas indebidas comprometan la seguridad, continuidad o resiliencia de las infraestructuras críticas y servicios esenciales.

Artículo 4. Definiciones: A los efectos de la presente Ley, sus normas complementarias, y sus reglamentos, se consideran las siguientes definiciones:

1. Activo Crítico: es todo bien, recurso, infraestructura, sistema, red, información, proceso o capacidad, de naturaleza física, digital, tecnológica o humana, cuya afectación o interrupción pueda generar un impacto grave en la seguridad nacional, la economía, el orden público, la continuidad de los servicios esenciales o el funcionamiento del Estado;
2. Amenaza Cibernética: es cualquier acción, intento o potencial incidente, de origen interno o externo, que mediante el uso de tecnologías de la información y las comunicaciones (TIC) busque vulnerar la confidencialidad, integridad, disponibilidad o control de los sistemas digitales, redes y procesos de operación de los servicios esenciales;
3. Amenaza Física: es toda acción, evento o condición, de origen humano, natural o tecnológico, con capacidad de causar daño, intrusión, sabotaje o interrupción mediante medios materiales o fuerza física, afectando la seguridad, integridad o continuidad de infraestructuras críticas y servicios esenciales;
4. Autoridad Sectorial: Entidad pública con competencia legal para regular, supervisar, fiscalizar y sancionar las actividades de un sector determinado, así como para dictar normas y otorgar las autorizaciones correspondientes dentro de su ámbito de competencia;
5. Ciberespacio Estratégico Nacional: es el conjunto de infraestructuras, sistemas, redes, servicios digitales, datos y flujos de información, públicos y privados, ubicados en Panamá o bajo su jurisdicción o interés estratégico, que permiten la generación, transmisión, procesamiento y almacenamiento de información mediante tecnologías de la información y la comunicación.;
6. Ciberdefensa: es la función estratégica del Estado orientada a prevenir, detectar, mitigar y responder a amenazas, ataques o incidentes físicos o cibernéticos que comprometan la seguridad nacional, la soberanía digital o la operación de las infraestructuras críticas y los servicios esenciales;
7. Ciberseguridad: es el conjunto de políticas, medidas y capacidades destinadas a proteger sistemas, redes, datos y servicios digitales frente a accesos no autorizados, alteraciones, daños o interrupciones que puedan afectar la confidencialidad, integridad, disponibilidad o continuidad de las infraestructuras críticas y los servicios esenciales;

8. Continuidad Operativa: es la capacidad de una infraestructura crítica u operador de servicios esenciales para mantener sus funciones indispensables sin interrupciones significativas, incluso frente a incidentes cibernéticos, fallas técnicas o situaciones de crisis;
9. Contratista: es toda persona natural o jurídica, pública o privada, que en virtud de un contrato o instrumento jurídico provee bienes, obras o servicios a un operador crítico, cuya actividad incide directa o indirectamente en la operación, seguridad, continuidad o resiliencia de una infraestructura crítica o servicio esencial;
10. Gestión Integral de Riesgos: es el conjunto sistemático y continuo de procesos para identificar, evaluar, tratar y monitorear riesgos físicos y cibernéticos que puedan afectar la seguridad, protección, resiliencia y continuidad de las infraestructuras críticas y los servicios esenciales;
11. Incidente Cibernético: es cualquier evento o acción no deseada, inesperada o maliciosa que afecta o intenta afectar la confidencialidad, integridad o disponibilidad de sistemas de información, redes, servicios digitales o datos, poniendo en riesgo la operación normal, la seguridad de la información o la continuidad de los servicios;
12. Incidente Cibernético Severo: todo evento de ciberseguridad que afecte o pueda afectar de forma debilitante, la operación, continuidad o seguridad de las infraestructuras críticas o servicios esenciales, ocasionando interrupciones relevantes, compromisos sustanciales de información, impactos económicos considerables o riesgos para la seguridad nacional;
13. Infraestructura Crítica: aquellas instalaciones, redes, sistemas, activos físicos o digitales, cuya perturbación pueda afectar gravemente la seguridad pública, la economía, el bienestar de la población, y la seguridad nacional;
14. Medidas de seguridad física y cibernética: son el conjunto de controles, acciones y procedimientos técnicos y organizativos destinados a prevenir, detectar, mitigar, responder y recuperar frente a amenazas o incidentes físicos o cibernéticos que afecten la integridad, disponibilidad, confidencialidad y continuidad de las infraestructuras críticas y los servicios esenciales;
15. Operador Crítico: es cualquier entidad pública o privada responsable de gestionar, administrar o garantizar el funcionamiento continuo y seguro de una infraestructura o servicio cuya interrupción afectaría gravemente la seguridad nacional, el orden público, la economía o el bienestar de la población;
16. Regulador Sectorial: es entidad pública con competencia legal para regular, supervisar y fiscalizar un sector o servicio determinado, y para dictar y hacer cumplir disposiciones técnicas o administrativas en materia de seguridad física y cibernética, continuidad operativa y protección de infraestructuras críticas y servicios esenciales;
17. Resiliencia: es la capacidad de una infraestructura crítica, servicio esencial, sistema, operador crítico, proveedor tecnológico y de telecomunicaciones, contratista y subcontratista, para resistir, absorber, adaptarse y recuperarse de incidentes cibernéticos, asegurando la continuidad de sus funciones críticas con el menor impacto posible;
18. Riesgo Cibernético: es la probabilidad de que un evento, vulnerabilidad o amenaza en el ciberespacio estratégico nacional, afecte la disponibilidad, integridad, confidencialidad o continuidad operativa de las infraestructuras críticas, los servicios esenciales o los sistemas de información relacionados, generando impactos técnicos, operativos, económicos o de seguridad nacional;

19. Riesgo Físico: es la probabilidad de que una amenaza física se materialice y cause un impacto adverso sobre un activo crítico, instalación, persona, proceso o servicio, considerando la combinación de la exposición, la vulnerabilidad y las consecuencias potenciales, pudiendo afectar la seguridad, integridad, disponibilidad y continuidad de las infraestructuras críticas y los servicios esenciales;
20. Sector Crítico: es el conjunto de actividades, servicios o áreas estratégicas cuya interrupción, degradación o afectación puede comprometer la seguridad nacional, el orden público, la economía, la salud, o la continuidad de los servicios esenciales del Estado;
21. Seguridad Nacional: es el conjunto de acciones, capacidades y políticas del Estado orientadas a proteger la soberanía, la integridad territorial, la estabilidad institucional, el bienestar de la población y el funcionamiento continuo de las infraestructuras críticas y servicios esenciales frente a amenazas internas o externas, incluyendo aquellas de naturaleza cibernética.
22. Servicios Esenciales: son las funciones críticas indispensables para el funcionamiento de la sociedad, cuya interrupción afectaría gravemente la continuidad de la economía nacional, el bienestar de la población, la seguridad nacional o la continuidad del Estado;
23. Subcontratista: es toda persona natural o jurídica, pública o privada, que por encargo del contratista principal ejecuta total o parcialmente obligaciones vinculadas al operador crítico, cuya actividad incide o puede incidir en la seguridad, operación o continuidad de una infraestructura crítica o servicio esencial.

Capitulo II
Gobernanza, Fiscalización y Régimen Sancionador.

Sección Primera.
Gobernanza.

Artículo 5. Gobernanza: La seguridad, protección y resiliencia de las infraestructuras críticas y los servicios esenciales se regirá por un modelo de gobernanza integral, estratégico y coordinado, bajo la dirección del Consejo Estratégico de Infraestructuras Críticas y Servicios Esenciales. Este modelo de gobernanza comprenderá:

1. La formulación de políticas y directrices estratégicas en materia de protección y seguridad;
2. La coordinación interinstitucional entre autoridades nacionales, sectoriales y reguladoras;
3. La articulación con el sector privado responsable de la operación de infraestructuras críticas y servicios esenciales;
4. La gestión integral de riesgos, incluyendo riesgos físicos, cibernéticos, ambientales, sanitarios y económicos;
5. La adopción de medidas orientadas a fortalecer la resiliencia y continuidad operativa frente a amenazas o incidentes.

La gobernanza establecida en la presente Ley se ejercerá sin perjuicio de las competencias constitucionales y legales de las entidades públicas y reguladores sectoriales.

Artículo 6. Creación, Naturaleza y Estructura: Créase el Consejo Estratégico de Infraestructuras Críticas y Servicios Esenciales, como órgano de alto nivel, de carácter estratégico y de coordinación

interinstitucional, responsable de dirigir la política nacional en materia de seguridad, protección y resiliencia de las Infraestructuras Críticas y los Servicios Esenciales. El Consejo ejercerá sus funciones a través de la siguiente estructura interna:

1. Comité Directivo, encargado de la dirección estratégica y la adopción de políticas y lineamientos nacionales;
2. Comité y Unidades Fiscalizadoras, responsables de la supervisión técnica y verificación del cumplimiento de la presente Ley y sus reglamentos;
3. Comisión Sancionadora, competente para conocer e imponer las sanciones administrativas previstas en esta Ley, con garantía del debido proceso.

Su organización, integración y funcionamiento serán desarrollados reglamentariamente.

Artículo 7. Comité Directivo: El Comité Directivo del Consejo Estratégico de Infraestructuras Críticas y Servicios Esenciales estará adscrito al sistema de seguridad del Estado, con enfoque de seguridad nacional, y será presidido por el Ministerio de la Presidencia. Estará integrado, y tendrán derecho a voz y voto los representantes, formalmente designados de las siguientes entidades:

1. Ministerio de la Presidencia,
2. Ministerio de Seguridad Pública,
3. Autoridad del Canal de Panamá,
4. Autoridad Nacional de los Servicios Públicos,
5. Autoridad Marítima de Panamá,
6. Autoridad de Innovación Gubernamental,
7. Servicio Nacional de Ciberdefensa,
8. Secretaría del Consejo de Seguridad,
9. Secretaría Nacional de Ciencia y Tecnología.

Cuando la naturaleza del riesgo o amenaza lo requiera, podrán ser convocadas otras autoridades, estamentos de seguridad o entidades públicas con competencia sectorial o técnica. Su organización, procedimientos y mecanismos de actuación serán desarrollados en el reglamento de la presente Ley.

Artículo 8. Competencias: El Consejo Estratégico ejercerá la coordinación y dirección estratégica interinstitucional, con las siguientes funciones:

1. Definir la política nacional de protección, seguridad y resiliencia de las infraestructuras críticas y servicios esenciales, con enfoque integral, preventivo y de seguridad nacional, abarcando riesgos físicos y cibernéticos,
2. Identificar, clasificar y priorizar infraestructuras críticas y servicios esenciales según riesgos, impactos y continuidad operativa,
3. Evaluar amenazas geopolíticas, estratégicas, incluidos riesgos físicos, ambientales, sanitarios, económicos y cibernéticos, que puedan afectar la continuidad de los servicios esenciales,
4. Aprobar lineamientos y estándares mínimos de seguridad, protección y continuidad que deben cumplir los operadores públicos y privados,
5. Coordinar la actuación interinstitucional de entidades competentes en seguridad, finanzas, ambiente, salud, comercio, industria y gestión gubernamental,

6. Establecer directrices para la gestión de crisis y la respuesta estratégica ante incidentes que afecten infraestructuras críticas o servicios esenciales,
7. Promover la asignación eficiente de recursos y priorización presupuestaria, en coordinación con el Ministerio de Economía y Finanzas,
8. Fomentar la cooperación nacional e internacional, incluyendo asistencia técnica, intercambio de información y buenas prácticas,
9. Supervisar la implementación de la política nacional, sin perjuicio de las competencias sectoriales y regulatorias,
10. Recomendar ajustes normativos y regulatorios para fortalecer la seguridad física y cibernética, la protección y la continuidad de las infraestructuras críticas y servicios esenciales,
11. Y demás competencias que se establezcan en el reglamento.

Sección Segunda
Comité y Unidades Fiscalizadoras.

Artículo 9. Naturaleza y Competencias: El Comité Fiscalizador es el órgano de carácter técnico encargado de dirigir y coordinar las actuaciones fiscalizadoras y de supervisión que las Unidades Fiscalizadoras, realicen en apego a lo establecido en la presente Ley y su reglamento.

Las Unidades Fiscalizadoras son las instancias de carácter interinstitucionales que ejecutarán las acciones y se encargarán de la supervisión, verificación y evaluación del nivel de cumplimiento de las obligaciones establecidas en la presente Ley y su reglamento.

Ambas instancias actuarán con independencia técnica y conforme a los principios de objetividad, proporcionalidad y coordinación interinstitucional.

Artículo 10. Composición del Comité y las Unidades Fiscalizadoras: El Comité Fiscalizador tendrá composición variable según el sector crítico involucrado y estará integrado, como mínimo, por:

1. Un representante designado del Comité Directivo del Consejo Estratégico, quien lo coordinará,
2. El ministerio o autoridad rectora del sector correspondiente,
3. El ente regulador sectorial,
4. Las autoridades técnicas que determine el reglamento.

Las Unidades Fiscalizadoras tendrán la composición que a consideración del sector crítico involucrado y lo que se establezca en el reglamento. Los procedimientos y mecanismos de actuación del Comité y las Unidades Fiscalizadoras se establecerán en el reglamento de la presente Ley.

Artículo 11. Competencias: Corresponde al Comité:

1. Realizar inspecciones, auditorías y evaluaciones de riesgo,
2. Verificar el cumplimiento de planes de seguridad y continuidad operativa,
3. Evaluar reportes de incidentes físicos o cibernéticos,
4. Emitir informes técnicos de incumplimiento,
5. Recomendar la apertura del procedimiento sancionador ante la Comisión Sancionadora,
6. Proponer medidas correctivas inmediatas cuando exista riesgo inminente,
7. Y las demás competencias que se establezcan en el reglamento.

Sección Tercera
Comisión Sancionadora.

Artículo 12. Creación y Naturaleza: Créase la Comisión Sancionadora en Materia de Infraestructuras Críticas y Servicios Esenciales, como órgano administrativo con competencia para conocer y decidir los procedimientos sancionadores derivados de los incumplimientos determinados conforme a esta Ley.

Artículo 13. Integración: La Comisión estará integrada por:

1. Un representante designado del Comité Directivo del Consejo Estratégico, quien la presidirá,
2. Un representante del ente regulador sectorial correspondiente,
3. Un representante del ministerio rector del sector.

Los procedimientos y mecanismos de actuación de la Comisión Sancionadora se establecerán en el reglamento de la presente Ley. Sus miembros deberán actuar con independencia, imparcialidad y sujeción estricta a la Ley.

Artículo 14. Competencias: Corresponde a la Comisión:

1. Admitir y conocer los expedientes remitidos por el Comité Fiscalizador,
2. Garantizar el derecho de defensa y el debido proceso,
3. Calificar las infracciones como leves, graves o muy graves,
4. Imponer las sanciones administrativas correspondientes,
5. Ordenar medidas correctivas o de supervisión reforzada,
6. Remitir antecedentes al Ministerio Público cuando existan indicios de delito.

Artículo 15. Procedimiento: El procedimiento sancionador se desarrollará conforme a:

1. Notificación formal de cargos,
2. Oportunidad para descargos y pruebas,
3. Audiencia administrativa cuando corresponda,
4. Resolución motivada,
5. Recursos administrativos conforme a la legislación vigente.

Sección Cuarta
Régimen de Infracciones y Sanciones.

Artículo 16. Ámbito y Potestad Sancionadora: Los operadores públicos y privados de infraestructuras críticas y servicios esenciales, así como sus proveedores, contratistas y subcontratistas, serán responsables por el incumplimiento de las obligaciones establecidas en esta Ley para garantizar la protección, seguridad física y cibernética, continuidad operativa y resiliencia.

La facultad de instruir, investigar e imponer sanciones corresponderá al Consejo Estratégico, a través del Comité Fiscalizador y la Comisión Sancionatoria, sin perjuicio de la cooperación técnica de los reguladores sectoriales.

Artículo 17. Clasificación de las Infracciones: Las infracciones se clasifican en leves, graves y muy graves, atendiendo al nivel de riesgo o impacto real o potencial sobre la seguridad nacional, la economía, el bienestar de la población o la continuidad del Estado.

Artículo 18. Infracciones Leves: Constituyen infracciones leves los incumplimientos formales o documentales que no generen riesgo directo a la seguridad física o cibernética.

Sanciones: amonestación escrita o multa de B/.1,000 a B/.25,000.

Artículo 19. Infracciones Graves: Constituyen infracciones graves:

1. No implementar o mantener los controles mínimos de seguridad física o cibernética exigidos,
2. Obstaculizar la supervisión o auditoría de la autoridad del Comité Fiscalizador,
3. No notificar oportunamente incidentes físicos o cibernéticos relevantes,
4. Incumplir instrucciones técnicas emitidas ante situaciones de riesgo,
5. No gestionar vulnerabilidades advertidas por la autoridad.

Sanciones: multa de B/.25,001 a B/.100,000, suspensión temporal de actividades no esenciales o imposición de plan de remediación supervisado.

Artículo 20. Infracciones Muy Graves: Constituyen infracciones muy graves:

1. Conductas u omisiones que provoquen o contribuyan a incidentes físicos, cibernéticos o híbridos que afecten gravemente infraestructuras críticas o servicios esenciales,
2. Negarse a colaborar con la autoridad en situaciones de emergencia,
3. Alterar, ocultar o destruir información relevante para la gestión de riesgos,
4. Incumplir medidas obligatorias que comprometan la seguridad nacional o la continuidad del servicio,
5. Exponer deliberadamente instalaciones, sistemas o redes críticas por dolo o negligencia grave.

Sanciones: multa de B/.100,001 a B/.500,000, suspensión total o parcial de operaciones, inhabilitación temporal o revocatoria del permiso de operación.

Artículo 21. Agravantes y Atenuantes: Serán agravantes la reincidencia en 24 meses, la afectación severa a la seguridad nacional o la obstrucción a la autoridad.

Serán atenuantes la notificación voluntaria del riesgo o incidente, la cooperación efectiva y la adopción previa de medidas superiores a las exigidas.

Artículo 22. Medidas Preventivas y Cautelares: Cuando exista riesgo inminente o grave para la seguridad física, cibernética o continuidad del servicio, la autoridad podrá ordenar medidas inmediatas, incluyendo suspensión temporal de áreas o sistemas vulnerables, intervención técnica o implementación urgente de controles.

Artículo 23. Procedimiento Sancionador: Las sanciones se impondrán mediante procedimiento administrativo que garantice el debido proceso. Podrán adoptarse medidas cautelares ante riesgo grave o inminente. La graduación de la sanción atenderá a la gravedad, impacto, intencionalidad, reincidencia y cooperación del infractor. La prescripción será regulada reglamentariamente.

Sección Quinta
Grupos de Apoyo Técnico Especializado.

Artículo 24. Creación: El Consejo Estratégico podrá conformar Grupos de Apoyo Técnico Especializado, permanentes o ad hoc, para asistir al Comité Fiscalizador o a la Comisión Sancionadora en materias técnicas complejas.

Artículo 25. Funciones: Los Grupos de Apoyo Técnico tendrán las siguientes funciones:

1. Realizar análisis forenses digitales o técnicos,
2. Emitir dictámenes especializados,
3. Evaluar impactos sistémicos y riesgos estructurales,
4. Apoyar en la gestión técnica de incidentes de alto impacto.

Sus dictámenes tendrán carácter técnico y no vinculante.

Sección Sexta
Trasparencia y Control Estratégico.

Artículo 26. Transparencia y Control Estratégico: Los operadores de infraestructuras críticas y servicios esenciales deberán declarar y mantener actualizada la información sobre su estructura de propiedad y beneficiario final.

Todo cambio que afecte la seguridad, continuidad o integridad operativa deberá notificarse oportunamente.

El Consejo Estratégico, a través de su Comité Fiscalizador, podrá evaluar los riesgos que determinadas actividades, estructuras de propiedad, cambios de control o circunstancias operativas representen para la seguridad nacional o la continuidad del Estado, y adoptar medidas proporcionales de mitigación, incluyendo el condicionamiento, limitación o suspensión de operaciones cuando resulte estrictamente necesario. La omisión de información relevante o la presentación de información falsa o inexacta constituirá infracción conforme al régimen sancionador establecido en la presente Ley.

Artículo 27. Evaluación de Riesgo en Inversiones Estratégicas: El Consejo Estratégico, a través del Comité Fiscalizado, podrá evaluar adquisiciones, fusiones, cesiones o cambios de control que involucren infraestructuras críticas o servicios esenciales y que representen riesgos para la seguridad nacional o la soberanía tecnológica, pudiendo imponer medidas de mitigación, condicionar o suspender la operación en casos excepcionales.

Artículo 28. Propiedad, Control o Influencia Extranjera: La propiedad, el control o la influencia extranjera sobre infraestructuras críticas o servicios esenciales constituirá un factor de evaluación de riesgo estratégico, cuando pueda afectar la seguridad nacional, la soberanía tecnológica, la continuidad del Estado o la prestación ininterrumpida de servicios esenciales.

Se entenderá por influencia extranjera toda capacidad directa o indirecta de incidir en decisiones estratégicas, acceso a información sensible, operación técnica o control efectivo de activos críticos.

Artículo 29. Obligación de Notificación de Operaciones Estratégicas: Deberán ser notificadas al Consejo Estratégico, previo a su ejecución:

1. Las adquisiciones, fusiones o cambios de control que involucren operadores de infraestructuras críticas o servicios esenciales;
2. La adquisición directa o indirecta de participación accionaria significativa;
3. Los acuerdos que otorguen control operativo, tecnológico o de gestión;

4. Los contratos que impliquen acceso remoto, administración tecnológica o tratamiento de información estratégica desde el extranjero.

El reglamento establecerá los umbrales y criterios de aplicación.

Artículo 30. Evaluación de Riesgo Estratégico: Recibida la notificación, el Consejo Estratégico, con apoyo del Comité Fiscalizador y los organismos de seguridad del Estado, realizará una evaluación técnica de riesgo basada en:

1. Impacto en la seguridad nacional;
2. Nivel de control o influencia efectiva;
3. Acceso a información sensible o sistemas críticos;
4. Dependencia tecnológica o de suministro;
5. Riesgo geopolítico o coerción estatal extranjera.

La evaluación deberá ser objetiva, técnica y proporcional.

Artículo 31. Medidas de Mitigación: Cuando se identifique un riesgo estratégico, la autoridad podrá:

1. Autorizar la operación con condiciones;
2. Exigir medidas de mitigación;
3. Establecer restricciones de acceso a información clasificada;
4. Requerir estructuras de gobernanza específicas;
5. Exigir localización de datos o infraestructura en territorio nacional;
6. Recomendar la suspensión o prohibición en casos excepcionales debidamente motivados.

Las medidas deberán ser proporcionales al nivel de riesgo identificado.

Artículo 32. Transparencia de Beneficiarios Finales: Los operadores de infraestructuras críticas y servicios esenciales, así como toda persona natural o jurídica que participe directa o indirectamente en licencias, contratos, concesiones, arrendamientos o asociaciones público-privadas vinculadas a dichas infraestructuras o servicios, estarán obligados a:

1. Identificar, verificar y mantener actualizada la información sobre sus propietarios efectivos y beneficiarios finales durante toda la vigencia del vínculo jurídico correspondiente. No serán oponibles disposiciones de secreto corporativo, fiduciario o contractual que impidan la identificación del beneficiario final, aun cuando intervengan Estados extranjeros, entidades estatales extranjeras, organismos internacionales, fondos soberanos o figuras similares.
2. Declarar las estructuras de propiedad indirecta, fiduciaria o cualquier otro mecanismo que permita ejercer control o influencia significativa.
3. Informar cualquier vínculo, participación o relación de control con gobiernos extranjeros o entidades estatales extranjeras.
4. Presentar la información prevista en el presente artículo al Consejo Estratégico y al regulador para su verificación en el Registro de Beneficiarios Finales de la República de Panamá, la cual estará disponible, conforme a la ley, para el Consejo Estratégico de Infraestructuras Críticas y Servicios Esenciales, los reguladores sectoriales.

La omisión, ocultamiento o falsedad en la información requerida constituirá infracción grave o muy grave, sin perjuicio de las responsabilidades administrativas, civiles o penales que correspondan.

Capítulo III
Servicio Nacional de Ciberdefensa (SNC).

Artículo 33. Servicio Nacional de Ciberdefensa (SNC): Créase el Servicio Nacional de Ciberdefensa (SNC) como entidad especializada responsable de la ciberdefensa nacional y la protección del ciberespacio estratégico nacional, adscrita al Ministerio de Seguridad Pública y bajo la autoridad superior del Presidente de la República.

El Servicio Nacional de Ciberdefensa (SNC), formará parte de la Fuerza Pública, tendrá carácter permanente, estructura técnica especializada con componentes civiles y operativos, y estará sujeto a régimen de carrera profesional y disciplina especial conforme a la ley.

Artículo 34. Dirección y Estructura Organizativa: El Servicio Nacional de Ciberdefensa (SNC) estará dirigido por un Director General y un Subdirector General, de libre nombramiento y remoción del Presidente de la República. Sus requisitos y funciones serán establecidos en el reglamento.

El Servicio Nacional de Ciberdefensa (SNC), contará con la estructura administrativa, técnica y operativa necesaria para el cumplimiento de sus fines, incluyendo un Centro de Operaciones de Ciberdefensa (C-SOC), un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), un Equipo de Tarea Conjunta contra el Ciberdelito (ETCC), así como las demás dependencias que se establezcan reglamentariamente.

Artículo 35. Competencias: El Servicio Nacional de Ciberdefensa (SNC) tendrá las siguientes competencias:

1. Dirigir y ejecutar la ciberdefensa nacional frente a amenazas que afecten la seguridad del Estado,
2. Proteger el ciberespacio estratégico nacional, estratégico para el Estado, y las infraestructuras críticas frente a ataques o incidentes cibernéticos,
3. Detectar, prevenir, contener y neutralizar amenazas cibernéticas de alto impacto
4. Coordinar la respuesta nacional ante incidentes cibernéticos graves o de carácter estratégico,
5. Operar un Centro Nacional de Operaciones de Ciberdefensa (C-SOC) y un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT),
6. Realizar análisis de inteligencia cibernética y evaluación de riesgos estratégicos,
7. Apoyar técnicamente al Consejo Estratégico, al Comité Fiscalizador, y a la Comisión Sancionadora, en la investigación de ciberdelitos que afecten la seguridad nacional,
8. Emitir directrices técnicas obligatorias en materia de ciberdefensa para entidades públicas estratégicas,
9. Promover la resiliencia y continuidad operativa frente a incidentes cibernéticos, que puedan afectar la seguridad nacional,
10. Coordinar, colaborar y apoyar a otros CSIRT, de los sectores públicos y privados,
11. Coordinar cooperación internacional en materia de ciberdefensa,
12. Y demás competencias que se establezcan en el reglamento.

Artículo 36. Régimen Disciplinario Especial del Personal: El personal del Servicio Nacional de Ciberdefensa (SNC), estará sujeto a un régimen disciplinario especial, acorde con la naturaleza estratégica, confidencial y de seguridad nacional de sus funciones.

Dicho régimen regulará la clasificación de faltas leves, graves y muy graves, las sanciones aplicables y el procedimiento disciplinario correspondiente, conforme a la ley y su reglamento.

Artículo 37. Protección Funcional del Personal Técnico de Ciberdefensa: El personal técnico, operativo y analítico del Servicio Nacional de Ciberdefensa (SNC), gozará de protección funcional para garantizar el ejercicio seguro, independiente y eficaz de sus funciones, especialmente en operaciones críticas, respuesta a incidentes graves o manejo de información clasificada.

Esta protección comprenderá asistencia legal institucional, respaldo administrativo por actuaciones realizadas en cumplimiento del deber y salvaguardas frente a presiones, amenazas o injerencias externas, conforme a lo que establezca el reglamento.

Artículo 38. Régimen Financiero: El Servicio Nacional de Ciberdefensa (SNC) se financiará con recursos del Presupuesto General del Estado, asignados al Ministerio de Seguridad Pública, aportes extraordinarios, cooperación internacional, e ingresos por servicios especializados.

La administración y ejecución de estos recursos se regirá por las normas de gestión financiera pública y por las disposiciones especiales que establezca el reglamento.

Capítulo IV
Sectores Críticos, Infraestructuras Críticas y Servicios Esenciales.

Artículo 39. Sectores Críticos: Esta Ley reconoce y establece como sectores críticos, los siguientes:

1. Sector Salud y Emergencias,
2. Sector Alimentación y Agricultura,
3. Sector Energía,
4. Sector Agua y Saneamiento,
5. Sector Transporte y Logística,
6. Sector Tecnología de la Información, telecomunicaciones y cables submarinos,
7. Sector Financiero y Seguros,
8. Sector Crítico Industrial,
9. Sector Crítico Comerciales,
10. Sector Servicios Gubernamentales y Administración Pública,
11. Sector Seguridad Pública y Defensa Nacional.

Artículo 40. Creación del Catálogo Nacional de Infraestructuras Críticas: Se crea el Catálogo Nacional de Infraestructuras Críticas y Servicios Esenciales, como instrumento oficial del Estado para la identificación, clasificación y priorización de los activos, sistemas, redes, instalaciones y servicios cuya afectación pueda generar un impacto significativo en la seguridad nacional, la economía, la salud pública, el orden social o la continuidad del Estado. El Catálogo tendrá carácter estratégico y será administrado conforme a lo dispuesto en la presente Ley.

Artículo 41. Administración del Catálogo Nacional de Infraestructuras Críticas: El Catálogo Nacional será administrado por el Consejo Estratégico de Infraestructuras Críticas y Servicios Esenciales, con apoyo técnico de las autoridades y reguladoras sectoriales.

La información contenida en el Catálogo estará sujeta a medidas especiales de custodia, control de acceso y protección.

Artículo 42. Criterios de Identificación y Clasificación: La inclusión de una infraestructura o servicio en el Catálogo Nacional se realizará conforme a criterios objetivos que consideren, entre otros:

1. El nivel de impacto potencial en la seguridad nacional,
2. La afectación a la economía o estabilidad financiera del país,
3. La interrupción significativa de servicios esenciales a la población,
4. La interdependencia con otros sectores críticos,
5. La exposición a amenazas físicas, ambientales o cibernéticas,
6. El grado de sustitución o redundancia disponible,

La reglamentación desarrollará la metodología de evaluación y clasificación.

Artículo 43. Criterios de Clasificación: La identificación y clasificación de infraestructuras críticas y servicios esenciales se basará en criterios técnicos tales como:

1. Impacto y nivel de dependencia en la economía, la seguridad nacional, el bienestar de la población, y la continuidad del Estado;
2. Impacto en la continuidad de los servicios públicos esenciales,
3. Grado de vulnerabilidad y exposición a riesgos cibernéticos,
4. Efecto cascada o afectación transversal a múltiples sectores,
5. Importancia estratégica para el funcionamiento del Estado.

Los criterios específicos, metodologías de evaluación y parámetros de clasificación serán desarrollados en el reglamento de esta Ley.

Artículo 44. Naturaleza Confidencial del Catálogo Nacional: La información contenida en el Catálogo Nacional de Infraestructuras Críticas y Servicios Esenciales tendrá carácter confidencial o de seguridad nacional cuando su divulgación pueda comprometer la protección, operación, continuidad o resiliencia de dichos activos.

No obstante, el Consejo Estratégico podrá divulgar información general o listados sectoriales agregados, siempre que no se identifiquen vulnerabilidades específicas, capacidades operativas sensibles u otros elementos cuya exposición represente un riesgo estratégico.

La clasificación, acceso, custodia y tratamiento de la información se regirán por los principios de necesidad, proporcionalidad y reserva, conforme a la legislación vigente en materia de transparencia y seguridad nacional.

El Catálogo Nacional será objeto de revisión y actualización periódica, o cuando cambios tecnológicos, operativos, estructurales o de riesgo así lo ameriten.

Capítulo V
Obligaciones de los Operadores Críticos, Proveedores, Contratistas y Subcontratistas.

Sección Primera

Obligaciones de los Operadores Críticos.

Artículo 45. Obligaciones de los Operadores Críticos: Los operadores críticos públicos y privados estarán obligados a:

1. Seguridad y Continuidad: Garantizar la seguridad, protección y continuidad operativa de las infraestructuras críticas y servicios esenciales bajo su gestión;
2. Gestión Integral de Riesgos: Identificar, evaluar y mitigar riesgos físicos, cibernéticos e híbridos que puedan afectar activos, funciones o servicios críticos, incluyendo a proveedores y contratistas;
3. Medidas y Controles: Implementar medidas mínimas de seguridad física y cibernética, proporcionales al nivel de riesgo y conforme a los lineamientos presentes en esta Ley, su reglamentos y demás directrices.
4. Prevención, Respuesta y Recuperación: Establecer mecanismos integrales de prevención, detección, respuesta y recuperación ante incidentes, incluyendo planes de continuidad operativa y pruebas periódicas de eficacia;
5. Notificación y Cooperación: Informar oportunamente al Consejo Directivo, y otras autoridades competentes, sobre incidentes de alto impacto y colaborar en auditorías, evaluaciones y acciones de coordinación, respetando la confidencialidad;
6. Capacitación y Cumplimiento: Formar a su personal, promover la cultura de seguridad y resiliencia, y cumplir con las disposiciones legales, reglamentarias y técnicas aplicables;
7. Contar con programas integrales de gestión de riesgos físicos y cibernéticos, seguridad, continuidad operativa, cumplimiento normativo, debida diligencia sobre beneficiarios finales y control extranjero, gestión de terceros, integridad y antisoborno, así como capacitación permanente;
8. Presentar anualmente al Consejo Estratégico, un informe consolidado sobre su nivel de riesgo y resiliencia, incidentes relevantes, cumplimiento de obligaciones, actualización de beneficiarios finales y estado de sus programas de seguridad e integridad;
9. Y demás obligaciones que se establezcan en el reglamento.

Sección Segunda
Obligaciones de los Proveedores, Contratistas y Subcontratistas.

Artículo 46. Obligaciones: Los proveedores tecnológicos y de telecomunicaciones, contratistas y subcontratistas que presten servicios, suministren tecnologías o ejecuten actividades vinculadas directa o indirectamente con la operación, seguridad o continuidad de infraestructuras críticas y servicios esenciales, estarán obligados a:

1. Cumplimiento de Seguridad y Continuidad: Implementar y mantener medidas de seguridad física y cibernética según los lineamientos y estándares establecidos por el operador y el Consejo Estratégico;
2. Gestión de Riesgos: Identificar, evaluar y mitigar riesgos físicos, cibernéticos e híbridos asociados a los servicios o productos que proveen;

3. Notificación de Incidentes: Informar de manera inmediata al operador crítico sobre incidentes o anomalías que puedan afectar la seguridad, continuidad o resiliencia de la infraestructura o servicio esencial;
4. Cooperación y Transparencia: Facilitar auditorías, inspecciones, evaluaciones y toda información requerida por el operador o por el Consejo Estratégico, respetando niveles de confidencialidad;
5. Planificación y Pruebas de Resiliencia: Colaborar en planes de continuidad operativa, recuperación ante incidentes y pruebas de eficacia de las medidas de seguridad implementadas;
6. Capacitación y Cultura de Seguridad: Garantizar que su personal reciba formación adecuada y mantenga prácticas de seguridad y resiliencia alineadas con los objetivos del operador y la ley;
7. Cumplimiento Normativo: Observar estrictamente todas las disposiciones legales, reglamentarias y técnicas aplicables a la operación de infraestructuras críticas y servicios esenciales;
8. Implementar programas proporcionales de gestión de riesgos físicos y cibernéticos, continuidad operativa, cumplimiento normativo, debida diligencia sobre beneficiarios finales y control o influencia extranjera, gestión de terceros, integridad y antisoborno, así como capacitación de su personal;
9. Remitir anualmente al operador crítico y, cuando corresponda, al Consejo Estratégico, un informe consolidado sobre cumplimiento, incidentes relevantes, riesgos identificados, actualización de beneficiarios finales y estado de sus programas de seguridad e integridad;
10. Y demás obligaciones que se establezcan en el reglamento.

Estas obligaciones son complementarias y no sustitutivas de las responsabilidades del operador crítico, y su alcance será proporcional al nivel de acceso, impacto y criticidad de los servicios o tecnologías suministradas.

Sección Tercera
Medidas de Seguridad Física y Cibernética

Artículo 47. Medidas de Seguridad Física y Cibernética: Los operadores críticos, proveedores, contratistas y subcontratistas deberán implementar medidas de seguridad física y cibernética, preventivas, detectivas, reactivas y correctivas, proporcionales al nivel de riesgo y criticidad, incluyendo:

1. Seguridad Física: control de accesos, vigilancia, protección perimetral, patrullaje, protocolos ante incidentes, protección de personas y activos, planes de contingencia y sistemas integrados de control;
2. Seguridad Cibernética: gestión de accesos y privilegios, monitoreo continuo, protección de redes y sistemas operativos, gestión de vulnerabilidades, respaldo y recuperación de información, respuesta a incidentes y segregación de entornos críticos;
3. Medidas Transversales: integración física y cibernética, capacitación del personal, documentación y mejora continua, coordinación con autoridades y cumplimiento de lineamientos técnicos.
4. Y demás medidas que se establezcan en el reglamento.

Las medidas deberán actualizarse periódicamente según la evolución de las amenazas, avances tecnológicos y criterios del Consejo Estratégico, sin perjuicio de adoptar medidas adicionales voluntarias para fortalecer la resiliencia y continuidad operativa.

Capítulo VI
Gestión Integral de Riesgos Físicos y Cibernéticos.

Artículo 48. Gestión Integral de Riesgos: Los operadores de infraestructuras críticas y servicios esenciales, así como sus proveedores, contratistas y subcontratistas que intervengan en su operación, soporte, seguridad o continuidad operativa, deberán gestionar de manera integral los riesgos físicos y cibernéticos, mediante la implementación y mantenimiento de marcos, modelos o estándares reconocidos que constituyan referencia técnica mínima para la protección, continuidad y resiliencia.

La gestión integral de riesgos comprenderá, como mínimo, las siguientes funciones:

1. Gobernar: Establecer una estructura de gobernanza que defina políticas, responsabilidades, procesos y mecanismos de supervisión orientados a la protección y continuidad operativa;
2. Identificar: Determinar y evaluar activos críticos, amenazas, vulnerabilidades, dependencias e interdependencias, así como escenarios de riesgo físicos y cibernéticos;
3. Proteger: Implementar controles y salvaguardas físicas, técnicas y organizativas para prevenir o mitigar riesgos e incidentes;
4. Detectar: Mantener capacidades de monitoreo y alerta temprana que permitan identificar oportunamente eventos o anomalías;
5. Responder: Activar planes y protocolos para la gestión y contención de incidentes, con la debida coordinación con el Consejo Estratégico, y las autoridades y reguladores sectoriales;
6. Recuperar: Restablecer oportunamente la operación y fortalecer la resiliencia mediante procesos de mejora continua;
7. Y demás funciones que se establezcan en el reglamento.

Las obligaciones específicas, requisitos técnicos y mecanismos de verificación serán desarrollados reglamentariamente. Los sujetos obligados deberán documentar y evidenciar el cumplimiento de estas disposiciones mediante auditorías, evaluaciones periódicas u otros mecanismos que determine el Consejo Estratégico.

Capítulo VII
Régimen General de Cumplimiento.

Artículo 49. Sistema de Cumplimiento en Seguridad Física y Cibernética: Los operadores de infraestructuras críticas y servicios esenciales deberán implementar y mantener un sistema interno de cumplimiento destinado a garantizar la observancia efectiva de las disposiciones de la presente Ley, sus reglamentos y los lineamientos emitidos por el Consejo Estratégico, así como la gestión continua de riesgos físicos y cibernéticos.

Artículo 50: Responsable de Cumplimiento: Los operadores críticos deberán designar un responsable de cumplimiento en materia de seguridad física y cibernética, con autonomía funcional y acceso directo al nivel directivo de la organización.

Artículo 51. Programa de Cumplimiento como Atenuante: La existencia efectiva, documentada y verificable de un programa integral de cumplimiento podrá considerarse circunstancia atenuante en la determinación de responsabilidades administrativas.

Artículo 52. Programas de Integridad y Antisoborno: Los operadores de infraestructuras críticas y servicios esenciales, así como sus proveedores, contratistas y subcontratistas, deberán:

1. Adoptar e implementar programas de cumplimiento e integridad que incluyan políticas antisoborno,
2. Establecer controles internos y mecanismos de debida diligencia en la selección de terceros,
3. Implementar canales de denuncia confidenciales,
4. Capacitar periódicamente a su personal en materia de ética y prevención de la corrupción,
5. Evaluar riesgos de corrupción como parte de la gestión integral de riesgos.
6. Y lo que se establezcan en el reglamento.

Capítulo VIII
Disposiciones Especiales.

Artículo 53. Obligación de Presentar Memoria Anual: El Consejo Estratégico de Infraestructuras Críticas y Servicios Esenciales deberá elaborar y presentar anualmente una Memoria Nacional sobre el Estado de la Seguridad y Resiliencia de las Infraestructuras Críticas y los Servicios Esenciales.

La Memoria tendrá carácter estratégico y constituirá instrumento oficial de evaluación y seguimiento de la política nacional en la materia.

Artículo 54. Destinatarios de la Memoria Anual: La Memoria Anual será presentada:

1. Al Presidente de la República;
2. Al Consejo de Gabinete;
3. Y podrá remitirse a la Asamblea Nacional para fines informativos, cuando corresponda.

Artículo 55. Contenido Mínimo de la Memoria Anual: La Memoria Anual deberá contener, como mínimo:

1. Evaluación general del nivel de riesgo nacional en materia de infraestructuras críticas y servicios esenciales;
2. Principales amenazas físicas y cibernéticas identificadas durante el período;
3. Estado de implementación de las Estrategias Nacionales;
4. Análisis agregado de incidentes relevantes;
5. Nivel de cumplimiento sectorial de obligaciones legales;
6. Evaluación de resiliencia y continuidad operativa;
7. Recomendaciones estratégicas y normativas;
8. Necesidades presupuestarias y de fortalecimiento institucional.

Artículo 56. Clasificación, Publicidad y Seguimiento de la Memoria Anual: La Memoria Anual podrá contener secciones clasificadas cuando su contenido esté relacionado con información sensible o de seguridad nacional.

El Consejo Estratégico podrá emitir una versión pública resumida que excluya información confidencial o estratégica.

El Consejo de Gabinete podrá emitir directrices estratégicas derivadas de la Memoria Anual, así como ordenar ajustes a la política nacional o a los lineamientos sectoriales.

Artículo 57. Obligación de Suministro de Información: Las entidades públicas y privadas que operen infraestructuras o servicios susceptibles de ser considerados críticos deberán suministrar la información técnica necesaria para su evaluación, conforme a los protocolos establecidos.

Artículo 58. Comités Sectoriales: La presente Ley promoverá la creación de Comités Sectoriales de Infraestructuras Críticas y Servicios Esenciales, como instancias de coordinación técnica y estratégica en cada sector considerado crítico conforme al Catálogo Nacional.

Los Comités Sectoriales tendrán como finalidad fortalecer la gestión integral de riesgos, la protección, la resiliencia y la continuidad operativa dentro de su respectivo ámbito sectorial.

Artículo 59. Intercambio Seguro de Información: El Estado promoverá un sistema seguro, oportuno y confiable de intercambio de información relacionada con amenazas, vulnerabilidades e incidentes que puedan afectar las Infraestructuras Críticas y los Servicios Esenciales.

El intercambio de información constituye un mecanismo esencial para la prevención, detección, respuesta y recuperación ante riesgos que afecten la seguridad nacional y la continuidad operativa del Estado.

Artículo 60. Sistema Seguro de Intercambio: El Consejo Estratégico, en coordinación con las autoridades y reguladores sectoriales en materia de seguridad y tecnología, establecerá mecanismos técnicos y protocolos de intercambio seguro de información, que garanticen:

1. Confidencialidad,
2. Integridad,
3. Disponibilidad,
4. Trazabilidad,
5. Control de acceso basado en niveles de clasificación.

Artículo 61. Obligación de Reporte: Los operadores públicos y privados de infraestructuras críticas y servicios esenciales deberán notificar al Consejo Estratégico los incidentes que:

1. Comprometan o puedan comprometer la continuidad operativa,
2. Generen afectación significativa a la seguridad física o cibernética,
3. Representen riesgos sistémicos o de alto impacto nacional.

La notificación deberá realizarse dentro de los plazos y conforme a los protocolos que establezca la reglamentación.

Artículo 62. Capacitación y Cultura de Seguridad: El Estado promoverá una cultura nacional de seguridad, protección y resiliencia orientada a la protección de las Infraestructuras Críticas y los Servicios Esenciales, basada en la prevención, la gestión integral de riesgos, la responsabilidad institucional y la conciencia ciudadana.

Artículo 63. Obligatoriedad de las Estrategias Nacionales: El Estado panameño adoptará y mantendrá vigentes las siguientes estrategias nacionales:

1. La Estrategia Nacional para la Seguridad, Protección y Resiliencia de las Infraestructuras Críticas y los Servicios Esenciales,
2. La Estrategia Nacional de Ciberseguridad,
3. La Estrategia Nacional de Ciberdefensa.

Estas estrategias constituyen instrumentos rectores de política pública en materia de seguridad nacional, gestión integral de riesgos, protección del Estado y continuidad operativa.

Artículo 64. Seguro Obligatorio para Incidentes Cibernéticos Severos: Los operadores públicos y privados clasificados como Infraestructuras Críticas de Nivel Estratégico Nacional o de Alto Impacto, conforme al Catálogo Nacional, deberán contratar y mantener vigente una póliza de seguro de riesgo cibernético destinada a cubrir los daños derivados de incidentes cibernéticos severos que comprometan la continuidad del servicio esencial, la estabilidad económica o la seguridad nacional.

Artículo 65. Alcances de un Incidente Cibernético Severo: Para efectos de la presente Ley, se considerará incidente cibernético severo aquel que:

1. Genere interrupción significativa del servicio esencial por un período superior al umbral que establezca la reglamentación;
2. Afecte de manera sustancial a un número relevante de usuarios o a sectores interdependientes;
3. Comprometa información estratégica o clasificada;
4. Produzca impacto económico significativo o riesgo sistémico;
5. Ponga en peligro la seguridad nacional.

La reglamentación desarrollará los criterios técnicos y métricas de severidad.

Artículo 66. Cobertura Mínima Obligatoria: La póliza deberá cubrir, como mínimo:

1. Interrupción o paralización del servicio esencial;
2. Costos de recuperación tecnológica y restauración de sistemas;
3. Investigación forense digital y contención del incidente;
4. Responsabilidad frente a terceros afectados;
5. Gestión de crisis y comunicación institucional;
6. Daños económicos derivados de afectación sistémica.

Artículo 67. Determinación del Monto Asegurado: El monto mínimo asegurado será determinado con base en:

1. El nivel de criticidad asignado en el Catálogo Nacional;
2. El análisis sectorial de impacto sistémico;
3. El volumen de operaciones y grado de interdependencia;
4. El riesgo residual identificado en las evaluaciones de seguridad.

El Consejo Estratégico, en coordinación con la Superintendencia de Seguros y Reaseguros de Panamá y las autoridades y reguladores sectoriales, establecerá los parámetros técnicos aplicables.

Artículo 68. Control Estratégico en Contrataciones Públicas: Toda contratación pública cuyo objeto comprenda la planificación, diseño, construcción, operación, mantenimiento, soporte tecnológico o seguridad física o cibernética de infraestructuras críticas o servicios esenciales se regirá por la Ley de Contrataciones Públicas y su reglamentación.

Sin perjuicio de lo anterior, dichas contrataciones deberán contar, previo a la adjudicación, con la apreciación estratégica del Consejo Estratégico en materia de Infraestructuras Críticas, limitada a la evaluación de riesgos para la seguridad nacional, la continuidad operativa, la soberanía tecnológica y la seguridad de la cadena de suministro.

Cuando concurran razones debidamente motivadas de seguridad nacional, defensa, orden público o protección de información clasificada, podrán aplicarse procedimientos especiales o regímenes de excepción, garantizando en todo caso los principios de legalidad, responsabilidad y control posterior, en la medida compatible con la naturaleza de la contratación.

La omisión de la apreciación estratégica previa constituirá vicio del procedimiento conforme a la presente Ley

Artículo 69. Prohibición y verificación estratégica previa: En las contrataciones, concesiones, asociaciones público-privadas o cualquier modalidad de relación jurídica vinculada a infraestructuras críticas o servicios esenciales, la entidad contratante deberá verificar, como parte del control estratégico previo, que el proponente no se encuentre incurso en las siguientes prohibiciones:

1. Haber sido condenado mediante sentencia firme en la República de Panamá o en el extranjero, incluyendo sus propietarios efectivos y beneficiarios finales, por delitos de corrupción, blanqueo de capitales, delincuencia organizada o financiamiento del terrorismo;
2. Ser Estado, gobierno o entidad estatal objeto de sanciones internacionales reconocidas por la República de Panamá por violaciones graves y sistemáticas de derechos humanos;
3. Ser Estado, gobierno o entidad estatal que haya sido declarado por ley formal de la República como adversario estratégico o respecto del cual exista situación jurídica de hostilidad reconocida por el Estado panameño.

La verificación de estas prohibiciones formará parte de la apreciación estratégica previa emitida por el Consejo Estratégico en materia de Infraestructuras Críticas.

Las prohibiciones previstas en este artículo son de orden público, no admiten excepciones ni mecanismos sustitutivos, y su incumplimiento producirá la nulidad absoluta del acto o contrato, sin perjuicio de las responsabilidades civiles, administrativas y penales correspondientes.

Artículo 70. Cumplimiento de estándares de ciberseguridad y seguridad de la cadena de suministro: Los proveedores de tecnologías de la información, comunicaciones y telecomunicaciones, que utilicen, integren o suministren equipos o servicios de comunicaciones, deberán:

1. Registrarse e iniciar el proceso de evaluación para la certificación conforme a las normas de la Asociación de la Industria de Telecomunicaciones, (TIA, por sus siglas en inglés), relativa a ciberseguridad y seguridad de la cadena de suministro en el sector de tecnologías de la información y las comunicaciones (TIC´s);

2. Acreditar ante el regulador competente la constancia de registro y el avance del proceso de evaluación correspondiente.

El regulador competente establecerá los plazos, parámetros de cumplimiento progresivo y medidas complementarias necesarias para garantizar la efectiva observancia de las normas de la Asociación de la Industria de Telecomunicaciones, (TIA, por sus siglas en inglés), u otros estándares equivalentes que aseguren la ciberseguridad y la integridad de la cadena de suministro.

Los equipos o sistemas preexistentes que no cumplan con los estándares exigidos podrán mantenerse en operación únicamente hasta el plazo que determine el regulador, quien deberá fijar un cronograma de adecuación obligatoria.

El incumplimiento de estas obligaciones dará lugar a la imposición de las sanciones administrativas previstas en la presente Ley, sin perjuicio de las responsabilidades civiles o penales a que hubiere lugar.

Capítulo IX
Disposiciones Transitorias y Finales.

Artículo 71. Transición: Los operadores críticos, autoridades reguladoras, proveedores, contratistas y subcontratistas, dispondrán de un plazo de doce (12) meses contados desde la fecha de su promulgación y entrada en vigencia, para realizar las adecuaciones y asignaciones de recursos económicos, que le permitan cumplir con lo dispuesto en la presente Ley, y su reglamento.

Artículo 72. Recursos: Las instituciones que forman parte de la gobernanza, fiscalización, régimen sancionatorio, o reguladores, deberán destinar los recursos presupuestarios para el debido cumplimiento de las competencias que se le atribuyen mediante la presente Ley, su reglamento y los cuales serán asignados de conformidad con las normas vigentes en materia presupuestaria.

Artículo 73. Reglamentación: El Órgano Ejecutivo reglamentará la presente Ley dentro del término de ciento ochenta (180) días calendario contados a partir de su promulgación, mediante Decreto Ejecutivo.

El reglamento desarrollará las disposiciones necesarias para su adecuada aplicación, incluyendo, entre otras materias:

1. Los criterios técnicos para la identificación y clasificación de infraestructuras críticas y servicios esenciales;
2. Los estándares mínimos de seguridad física, cibernética y de continuidad operativa;
3. Los mecanismos de coordinación interinstitucional;
4. Los procedimientos de gestión de crisis;
5. Los esquemas de intercambio seguro de información;
6. Los parámetros para la evaluación de riesgos y resiliencia;
7. Las obligaciones específicas de los sujetos regulados.

Sin perjuicio del reglamento general, las autoridades y reguladores sectoriales competentes podrán dictar reglamentos técnicos específicos en el ámbito de sus competencias, en concordancia con la presente Ley y su reglamento general.

Artículo 74. Entrada en Vigor: Esta Ley comenzará a regir doce (12) meses después de su promulgación en la Gaceta Oficial.

Artículo 75. Derogación: Quedan derogadas todas las disposiciones que sean contrarias a la presente Ley.

COMUNÍQUESE Y CÚMPLASE.

Dado en la ciudad de Panamá, a los ___ días del mes de _____ dos mil cinco (2026).