

**ANTEPROYECTO DE  
LEY ORGÁNICA DE GESTIÓN INTEGRADA Y  
TECNIFICACIÓN DE LA FRONTERA DE LA  
REPÚBLICA DOMINICANA**

**“FRONTERA INTELIGENTE RD”**

# CAPÍTULO I

## DISPOSICIONES GENERALES

### **Artículo 1.- Objeto.**

La presente ley tiene por objeto establecer el marco jurídico para la gestión integrada, tecnificación, interoperabilidad, trazabilidad y modernización progresiva de la frontera terrestre de la República Dominicana con la República de Haití, con la finalidad de fortalecer la soberanía nacional, la seguridad fronteriza, el control migratorio y aduanero, la bioseguridad, la protección ambiental, la facilitación del comercio legítimo y el desarrollo económico y social de la zona fronteriza.

La presente ley regulará, asimismo, los principios generales aplicables al diseño, implementación, operación, coordinación, supervisión, auditoría y evaluación de los sistemas tecnológicos utilizados para apoyar el ejercicio de las competencias públicas relacionadas con la gestión fronteriza.

**Párrafo I.-** La implementación de esta ley no implicará transferencia, sustitución ni modificación de las competencias atribuidas por la Constitución, las leyes y los reglamentos a los órganos y entes del Estado.

**Párrafo II.-** Ninguna disposición de esta ley podrá interpretarse como modificación de la delimitación territorial de la República Dominicana, de los tratados fronterizos vigentes ni de los compromisos internacionales válidamente asumidos por el Estado dominicano.

### **Artículo 2.- Ámbito de aplicación.**

Las disposiciones de esta ley serán aplicables a los órganos y entes de la Administración Pública que, conforme a la Constitución y las leyes, ejerzan competencias relacionadas directa o indirectamente con la seguridad, defensa, vigilancia, migración, aduanas, inteligencia, sanidad, agricultura, medio ambiente, telecomunicaciones, transformación digital, comercio, logística, infraestructura, desarrollo territorial o cualquier otra función pública vinculada con la gestión de la frontera terrestre dominico-haitiana.

El ámbito funcional de la presente ley comprenderá igualmente los sistemas, centros de comando, plataformas tecnológicas, redes de comunicaciones, bases de datos, instalaciones y demás infraestructuras ubicadas fuera de la zona fronteriza cuando sirvan directamente de apoyo a las operaciones reguladas por esta ley.

**Párrafo I.-** Los órganos constitucionales autónomos o extrapoderes participarán en los mecanismos de interoperabilidad, coordinación o intercambio de información únicamente

dentro de sus competencias constitucionales y legales y mediante los instrumentos jurídicos que correspondan, preservándose en todo momento su autonomía e independencia.

**Párrafo II.-** Las personas físicas o jurídicas de derecho privado quedarán sujetas a las disposiciones de esta ley únicamente en cuanto participen en procedimientos fronterizos regulados, utilicen infraestructuras o servicios sometidos a control estatal, sean contratistas o proveedores de componentes del sistema, o se encuentren sometidas a obligaciones expresamente establecidas por la legislación aplicable.

**Párrafo III.-** La presente ley será aplicada sin perjuicio de los regímenes especiales establecidos en materia migratoria, aduanera, militar, de inteligencia, sanitaria, ambiental, tributaria, de telecomunicaciones, protección de datos, contrataciones públicas y demás materias reguladas por leyes sectoriales.

### **Artículo 3.- Finalidades.**

Son finalidades de la presente ley:

- a) Fortalecer la capacidad del Estado dominicano para ejercer soberanía, vigilancia y control efectivo sobre su frontera terrestre;
- b) Integrar progresivamente las capacidades tecnológicas, operacionales e informativas de los órganos y entes competentes, sin menoscabo de sus respectivas atribuciones legales;
- c) Modernizar los procesos de identificación, registro, inspección, verificación, autorización, vigilancia y respuesta fronteriza;
- d) Promover la interoperabilidad segura entre sistemas estatales conforme al ordenamiento jurídico y a las normas técnicas gubernamentales aplicables;
- e) Garantizar la trazabilidad de las actuaciones administrativas y operacionales realizadas mediante los sistemas regulados por esta ley;
- f) Fortalecer la prevención, detección y respuesta frente al tráfico ilícito de migrantes, trata de personas, contrabando, narcotráfico, tráfico de armas, falsificación, evasión aduanera, delitos ambientales y demás actividades ilícitas cuya prevención o persecución corresponda legalmente a las autoridades competentes;
- g) Facilitar el movimiento legítimo y ordenado de personas, vehículos y mercancías a través de los puntos fronterizos habilitados;
- h) Mejorar la capacidad estatal para gestionar riesgos migratorios, aduaneros, sanitarios, fitosanitarios, zoonosarios, ambientales y de seguridad;
- i) Reducir los espacios de discrecionalidad administrativa no trazable y fortalecer los mecanismos de prevención, detección y control de actuaciones irregulares o corruptas;

- j) Garantizar que la utilización de biometría, inteligencia artificial, sistemas automatizados, cámaras, sensores, drones y demás tecnologías se realice con respeto a la Constitución, los derechos fundamentales y las leyes aplicables;
- k) Asegurar la continuidad operacional, resiliencia y ciberseguridad de la infraestructura tecnológica fronteriza;
- l) Promover la formalización, eficiencia y trazabilidad del comercio fronterizo legítimo;
- m) Contribuir al desarrollo económico, social, productivo, logístico, tecnológico y territorial de las provincias fronterizas;
- n) Optimizar el uso de los recursos públicos mediante la integración de sistemas existentes, evitando duplicidades tecnológicas e institucionales;
- o) Establecer mecanismos objetivos de evaluación, auditoría, control y rendición de cuentas sobre la política nacional de tecnificación fronteriza.

#### **Artículo 4.- Principios rectores.**

La interpretación, reglamentación y aplicación de la presente ley se regirá por los siguientes principios:

- a) Juridicidad. Toda actuación deberá someterse plenamente a la Constitución, las leyes, los reglamentos, los tratados aplicables y los principios generales del derecho;
- b) Soberanía nacional. La utilización de tecnología fronteriza estará orientada a fortalecer la capacidad del Estado dominicano para proteger su territorio, independencia, seguridad e intereses nacionales;
- c) Competencia institucional. Ningún sistema tecnológico podrá modificar, transferir o sustituir las atribuciones legalmente otorgadas a una autoridad pública;
- d) Coordinación interinstitucional. Los órganos competentes deberán cooperar e intercambiar información dentro de los límites de sus atribuciones, procurando una actuación estatal coherente y articulada;
- e) Interoperabilidad segura. Los sistemas deberán diseñarse para intercambiar información de manera controlada, estandarizada, verificable y segura, conforme a las normas técnicas gubernamentales aplicables;
- f) No duplicación. Antes de desarrollar o adquirir una nueva plataforma deberá evaluarse la posibilidad de utilizar, integrar o ampliar sistemas estatales existentes;
- g) Proporcionalidad. Las medidas tecnológicas y operacionales deberán ser adecuadas, necesarias y proporcionales a la finalidad legítima perseguida;

- h) Respeto de los derechos fundamentales. La tecnificación fronteriza deberá ejecutarse respetando la dignidad humana, igualdad, intimidad, protección de datos, debido proceso y demás derechos constitucionalmente reconocidos;
- i) No discriminación. Ninguna actuación automatizada o asistida tecnológicamente podrá fundamentar un trato adverso exclusivamente en características raciales, étnicas, religiosas, políticas, apariencia física u otras condiciones constitucionalmente protegidas;
- j) Finalidad y minimización de datos. Solo deberán recopilarse, consultarse, intercambiarse y conservarse los datos necesarios y pertinentes para finalidades legítimas expresamente determinadas;
- k) Seguridad por diseño. Todo componente tecnológico deberá incorporar desde su concepción medidas adecuadas de seguridad física, lógica y cibernética;
- l) Privacidad por diseño. Los sistemas que procesen datos personales deberán incorporar medidas de protección desde las etapas de diseño, contratación, desarrollo e implementación;
- m) Protección reforzada de datos biométricos. La información biométrica utilizada en los sistemas regulados por esta ley estará sometida a controles reforzados de acceso, seguridad, trazabilidad y utilización;
- n) Control humano de decisiones de alto impacto. Ninguna decisión estatal que produzca efectos restrictivos significativos sobre derechos podrá sustentarse exclusivamente en una decisión automatizada, sin la intervención de la autoridad legalmente competente;
- o) Trazabilidad. Toda actuación digital relevante deberá permitir determinar su origen, autor, fecha, hora, sistema utilizado y modificaciones realizadas;
- p) Integridad de la información. Los registros deberán protegerse contra alteraciones, destrucciones, sustituciones o manipulaciones no autorizadas;
- q) Neutralidad tecnológica. La ley y sus reglamentos establecerán requisitos funcionales y de seguridad evitando dependencia innecesaria de marcas, fabricantes o tecnologías propietarias;
- r) Gestión basada en riesgo. La asignación de controles, recursos e inspecciones podrá considerar análisis objetivos de riesgo, sin que ello sustituya las garantías legales aplicables;
- s) Continuidad operacional. Los sistemas críticos deberán diseñarse con capacidad de respaldo, contingencia, recuperación y operación degradada;
- t) Transparencia compatible con la seguridad nacional. La gestión administrativa, presupuestaria y contractual estará sujeta a los principios de transparencia y rendición de

cuentas, sin perjuicio de las reservas de información legítimamente establecidas por la Constitución y las leyes;

- u) Responsabilidad. Toda autoridad, funcionario, contratista o proveedor responderá por sus actuaciones u omisiones conforme al régimen jurídico que le resulte aplicable;
- v) Desarrollo fronterizo sostenible. La seguridad, tecnificación e infraestructura deberán contribuir al desarrollo económico, social, productivo y ambientalmente sostenible de la zona fronteriza;
- w) Mejora continua. Los sistemas, procedimientos, modelos automatizados e indicadores deberán ser evaluados periódicamente y ajustados conforme a resultados, nuevas amenazas, cambios normativos y evolución tecnológica.

#### **Artículo 5.- Definiciones.**

Para los fines de aplicación de la presente ley se entenderá por:

- a) Alerta automatizada: Notificación generada total o parcialmente mediante reglas programadas, sensores, analítica de datos, inteligencia artificial u otros mecanismos tecnológicos que identifica una posible anomalía, riesgo o circunstancia que requiere verificación;
- b) Autoridad funcional del evento: Órgano o ente que, conforme a la Constitución y las leyes, posee la competencia principal para adoptar la decisión administrativa, operacional o técnica correspondiente a un determinado evento fronterizo;
- c) Control humano: Intervención efectiva de un funcionario o autoridad competente con capacidad jurídica y material para revisar información, evaluar una recomendación tecnológica, solicitar verificaciones adicionales y adoptar la decisión que corresponda;
- d) Datos biométricos: Datos personales obtenidos mediante un tratamiento técnico específico relativo a características físicas, fisiológicas o conductuales de una persona que permiten o contribuyen a su identificación o verificación individual, tales como huellas dactilares, características faciales u otros identificadores biométricos legalmente autorizados;
- e) Decisión automatizada: Resultado generado mediante un sistema tecnológico, algoritmo, modelo estadístico o sistema de inteligencia artificial con intervención humana inexistente o limitada;
- f) Decisión de alto impacto: Actuación o determinación pública capaz de producir efectos jurídicos o materiales significativos sobre una persona, particularmente cuando pueda conducir a detención, rechazo migratorio, deportación, incautación, sanción, restricción de derechos o consecuencias equivalentes;

- g) Evaluación secundaria: Procedimiento de revisión adicional realizado por la autoridad competente cuando una verificación inicial resulte inconclusa, produzca una alerta o requiera comprobaciones adicionales conforme a la legislación aplicable;
- h) Evento fronterizo: Hecho, actuación, tránsito, detección, operación, incidencia o circunstancia vinculada con personas, vehículos, mercancías, infraestructura, seguridad, sanidad, medio ambiente o gestión administrativa que requiera registro o intervención de una autoridad dentro del ámbito de esta ley;
- i) Frontera Inteligente RD: Modelo nacional de gestión integrada que combina infraestructura física, tecnología, interoperabilidad, coordinación institucional, análisis de riesgo, control, auditoría y desarrollo territorial para fortalecer la administración de la frontera terrestre dominico-haitiana;
- j) Identificador Único de Evento Fronterizo o IUEF: Código electrónico asignado a un evento para permitir su vinculación y trazabilidad entre actuaciones o sistemas, sin sustituir los números de expedientes internos que correspondan a cada institución;
- k) Infraestructura tecnológica fronteriza: Conjunto de equipos, redes, plataformas, centros de procesamiento, sensores, cámaras, radares, sistemas biométricos, lectores electrónicos, drones, sistemas de comunicaciones, energía de respaldo y demás componentes utilizados para apoyar la gestión fronteriza;
- l) Interoperabilidad: Capacidad jurídica, organizacional, semántica y técnica de los órganos, sistemas y plataformas para intercambiar y utilizar información de manera coordinada, segura y estandarizada, preservando las competencias y responsabilidades de cada institución;
- m) Sistema automatizado: Sistema tecnológico que ejecuta procesos, clasificaciones, verificaciones, recomendaciones o actuaciones mediante reglas programadas, algoritmos, modelos estadísticos o inteligencia artificial;
- n) Sistema Integrado de Gestión Fronteriza Dominicana o SIGFRO-RD: Arquitectura tecnológica e interinstitucional de naturaleza federada destinada a facilitar la interoperabilidad, coordinación, trazabilidad, intercambio de información y gestión de eventos fronterizos entre los organismos competentes, sin constituir una nueva persona jurídica ni sustituir los sistemas institucionales existentes;
- o) Trazabilidad: Capacidad de reconstruir de manera verificable el origen, secuencia, responsables, consultas, actuaciones, modificaciones, decisiones y resultados asociados a un evento, dato o procedimiento;

- p) Verificación biométrica: Proceso técnico mediante el cual uno o más datos biométricos son comparados con una referencia legítimamente disponible para contribuir a confirmar la identidad de una persona;
- q) Punto fronterizo habilitado: Instalación, paso o lugar oficialmente autorizado por las autoridades competentes para realizar operaciones de entrada, salida, control migratorio, aduanero o de otra naturaleza legalmente prevista.

**Párrafo.-** Las definiciones contenidas en este artículo deberán interpretarse de manera armónica con las definiciones establecidas en las leyes sectoriales aplicables. En caso de que un término posea un significado técnico específico en una legislación especial para una materia determinada, prevalecerá dicha definición dentro del ámbito de aplicación de esa legislación.

## **CAPÍTULO II**

### **POLÍTICA NACIONAL Y SISTEMA INTEGRADO DE GESTIÓN FRONTERIZA DOMINICANA**

#### **Artículo 6.- Política Nacional de Gestión Integrada y Tecnificación Fronteriza.**

Se establece la Política Nacional de Gestión Integrada y Tecnificación Fronteriza, denominada para fines de identificación pública “Frontera Inteligente RD”, como marco permanente de planificación, coordinación, modernización, interoperabilidad, inversión, seguridad, control, evaluación y desarrollo de las capacidades del Estado vinculadas con la frontera terrestre dominico-haitiana.

La Política Nacional tendrá carácter transversal y deberá incorporarse, según corresponda, a los instrumentos de planificación, programación presupuestaria, inversión pública, transformación digital, seguridad y defensa, desarrollo fronterizo, comercio, logística, sanidad, protección ambiental y demás políticas públicas relacionadas con su ámbito de aplicación.

**Párrafo I.-** La Política Nacional se fundamenta en el carácter de supremo y permanente interés nacional que la Constitución reconoce a la seguridad y al desarrollo económico, social y turístico de la Zona Fronteriza, así como a su integración vial, comunicacional y productiva.

**Párrafo II.-** La Política Nacional deberá ejecutarse conforme a los principios establecidos en la presente ley y mediante el aprovechamiento prioritario, integración y fortalecimiento de las capacidades institucionales, tecnológicas y de infraestructura ya existentes en el Estado.

**Párrafo III.-** La denominación “Frontera Inteligente RD” tendrá fines programáticos y de identificación de la política pública y no implicará la creación de un órgano, ente, persona jurídica o dependencia administrativa independiente.

**Párrafo IV.-** La Política Nacional deberá ser objeto de evaluación y actualización periódica, conforme a los resultados alcanzados, la evolución tecnológica, los cambios en los riesgos fronterizos, las modificaciones normativas y las necesidades de desarrollo de la zona fronteriza.

#### **Artículo 7.- Creación del Sistema Integrado de Gestión Fronteriza Dominicana.**

Se crea el Sistema Integrado de Gestión Fronteriza Dominicana —SIGFRO-RD—, como mecanismo tecnológico, funcional e interinstitucional destinado a facilitar la interoperabilidad, coordinación, trazabilidad, intercambio seguro de información y gestión integrada de eventos relacionados con la frontera terrestre dominico-haitiana.

SIGFRO-RD constituirá uno de los instrumentos principales para la ejecución de la Política Nacional de Gestión Integrada y Tecnificación Fronteriza.

**Párrafo I.-** SIGFRO-RD integrará progresivamente, conforme al marco jurídico aplicable, los sistemas, servicios digitales, plataformas, dispositivos y fuentes de información necesarios para apoyar las funciones legalmente atribuidas a los órganos y entes competentes.

**Párrafo II.-** La integración a SIGFRO-RD no implicará sustitución de los sistemas institucionales existentes cuando estos puedan cumplir adecuadamente sus funciones e interoperar conforme a los estándares establecidos.

**Párrafo III.-** La incorporación de nuevos componentes deberá responder a necesidades técnicas, operacionales o jurídicas previamente identificadas y deberá evitar la creación de plataformas duplicadas o incompatibles con la arquitectura tecnológica del Estado.

**Párrafo IV.-** Los componentes de SIGFRO-RD deberán implementarse progresivamente conforme al Plan Maestro, la disponibilidad presupuestaria, los estudios técnicos correspondientes y los mecanismos de evaluación previstos en esta ley.

#### **Artículo 8.- Naturaleza y arquitectura de SIGFRO-RD.**

SIGFRO-RD tendrá naturaleza de sistema interinstitucional de coordinación tecnológica y operacional, sin personalidad jurídica, patrimonio, nómina ni presupuesto administrativo independiente de las instituciones que lo integran.

Su arquitectura será preferentemente federada y deberá permitir que cada órgano o ente mantenga la administración, custodia, actualización y responsabilidad sobre las fuentes de información que se encuentren legalmente bajo su competencia.

**Párrafo I.-** La interoperabilidad no requerirá la concentración indiscriminada de las bases de datos institucionales en un repositorio central cuando la finalidad pueda alcanzarse mediante consultas, intercambios o servicios seguros entre sistemas.

**Párrafo II.-** Cada institución continuará siendo responsable de administrar los datos y registros cuya producción o custodia le corresponda, garantizar su calidad, actualización, integridad y seguridad, determinar los niveles y condiciones de acceso dentro del marco jurídico aplicable, corregir los datos que resulten inexactos cuando corresponda y mantener los registros institucionales exigidos por la legislación sectorial.

**Párrafo III.-** La información intercambiada mediante SIGFRO-RD deberá limitarse a aquella que resulte necesaria, pertinente y jurídicamente autorizada para la finalidad específica de la consulta o actuación correspondiente.

**Párrafo IV.-** Las integraciones entre organismos del Poder Ejecutivo deberán utilizar, cuando resulte aplicable, la Plataforma Única de Interoperabilidad y cumplir las normas, estándares y lineamientos gubernamentales vigentes en materia de interoperabilidad, transformación digital, seguridad de la información y ciberseguridad.

**Párrafo V.-** Cuando por razones operacionales, de seguridad nacional, defensa, inteligencia, continuidad operacional o naturaleza técnica resulte necesaria una modalidad de interoperabilidad distinta, esta deberá contar con fundamento jurídico, controles de seguridad, documentación técnica y mecanismos de auditoría adecuados.

#### **Artículo 9.- Capacidades funcionales de SIGFRO-RD.**

Para el cumplimiento de sus finalidades, SIGFRO-RD podrá interconectar sistemas y servicios digitales de las instituciones competentes; consultar información proveniente de fuentes oficiales conforme a perfiles de acceso y finalidades autorizadas; registrar eventos fronterizos y vincular las actuaciones relacionadas con ellos; asignar el Identificador Único de Evento Fronterizo; generar y distribuir alertas; integrar información proveniente de dispositivos tecnológicos autorizados; apoyar procesos de análisis y clasificación de riesgos; facilitar el seguimiento y cierre de eventos; registrar actuaciones de usuarios y funcionarios; generar bitácoras de auditoría; elaborar estadísticas e indicadores; apoyar la continuidad operacional; detectar fallas de componentes; facilitar la supervisión del mantenimiento; coordinar operaciones interinstitucionales e incorporar mecanismos de análisis automatizado e inteligencia artificial dentro de los límites establecidos por esta ley.

**Párrafo I.-** Estas capacidades tendrán naturaleza instrumental y de apoyo y no conferirán a SIGFRO-RD competencia administrativa, migratoria, aduanera, militar, policial, investigativa, sancionadora o jurisdiccional propia.

**Párrafo II.-** La generación de una alerta, clasificación de riesgo, coincidencia biométrica, resultado algorítmico o recomendación automatizada no constituirá por sí misma una decisión administrativa definitiva ni una determinación de responsabilidad.

**Párrafo III.-** Las decisiones que produzcan efectos jurídicos sobre las personas, bienes, vehículos o mercancías deberán ser adoptadas por la autoridad competente conforme a la Constitución, las leyes, los reglamentos y los procedimientos aplicables.

**Artículo 10.- Preservación de competencias y autoridad funcional del evento.**

La implementación y operación de SIGFRO-RD se regirá por el principio de preservación de las competencias institucionales. Ningún órgano, funcionario, plataforma tecnológica, algoritmo o centro de coordinación podrá ejercer, mediante SIGFRO-RD, atribuciones que el ordenamiento jurídico haya conferido a otra autoridad.

Para cada evento se identificará la autoridad funcional competente, de acuerdo con la naturaleza de la actuación y las disposiciones constitucionales, legales y reglamentarias aplicables.

**Párrafo I.-** La Dirección General de Migración ejercerá las atribuciones relacionadas con el régimen migratorio; la Dirección General de Aduanas ejercerá las atribuciones aduaneras; el Ministerio de Defensa, las instituciones militares y CESFRONT ejercerán las funciones de defensa, seguridad y vigilancia fronteriza dentro de sus respectivas competencias; los órganos de inteligencia ejercerán únicamente las atribuciones legalmente asignadas; el Ministerio Público y los órganos de investigación competentes actuarán respecto de hechos que puedan constituir infracciones penales; y las autoridades sanitarias, agropecuarias, ambientales y demás organismos especializados ejercerán las competencias sectoriales que les atribuya el ordenamiento jurídico.

**Párrafo II.-** Cuando un mismo evento involucre competencias de dos o más instituciones, cada una ejercerá las atribuciones que le correspondan y coordinará sus actuaciones mediante SIGFRO-RD y los protocolos interinstitucionales aplicables.

**Párrafo III.-** La institución que detecte inicialmente un evento que corresponda total o parcialmente a la competencia de otra autoridad deberá comunicarlo oportunamente, sin perjuicio de las medidas urgentes que legalmente pueda adoptar dentro de sus propias atribuciones.

**Párrafo IV.-** El intercambio de información, la cooperación técnica, la utilización compartida de infraestructura o la participación conjunta en una operación no implicarán subordinación institucional ni transferencia tácita de competencias.

**Párrafo V.-** Ninguna credencial, constancia, identificación o registro generado por una institución distinta de la autoridad migratoria competente podrá conferir por sí mismo autorización de entrada, salida, permanencia, tránsito o regularidad migratoria cuando la legislación atribuya dicha decisión a la Dirección General de Migración.

**Párrafo VI.-** Ninguna alerta o recomendación emitida por SIGFRO-RD podrá utilizarse para obviar los procedimientos, autorizaciones, garantías o requisitos establecidos por la legislación sectorial aplicable.

## **CAPÍTULO III**

### **GOBERNANZA Y COORDINACIÓN INTERINSTITUCIONAL**

#### **Artículo 11.- Comisión Interinstitucional para la Frontera Inteligente.**

Se crea la Comisión Interinstitucional para la Frontera Inteligente —CIFI—, como instancia permanente de coordinación estratégica, seguimiento y evaluación de la Política Nacional de Gestión Integrada y Tecnificación Fronteriza y del Sistema Integrado de Gestión Fronteriza Dominicana —SIGFRO-RD—.

La Comisión estará vinculada al Ministerio de la Presidencia para fines de coordinación interinstitucional y no tendrá personalidad jurídica, patrimonio, nómina ni estructura administrativa independiente.

**Párrafo I.-** La Comisión no ejercerá competencias operacionales, migratorias, aduaneras, militares, policiales, de inteligencia, sanitarias, ambientales, regulatorias, investigativas, sancionadoras o jurisdiccionales atribuidas por la Constitución o las leyes a otras autoridades.

**Párrafo II.-** Las decisiones y acuerdos de la Comisión tendrán naturaleza de coordinación, planificación, estandarización y seguimiento. Cuando su ejecución requiera un acto administrativo, autorización, resolución, contratación, asignación presupuestaria o decisión reservada legalmente a una institución determinada, corresponderá a dicha institución adoptarlo conforme al procedimiento aplicable.

**Párrafo III.-** La creación de la Comisión no constituirá fundamento para establecer remuneraciones, dietas o estructuras administrativas adicionales.

#### **Artículo 12.- Integración.**

La Comisión estará presidida por el Ministerio de la Presidencia y tendrá como vicepresidente al Ministerio de Defensa.

La integrarán igualmente los titulares del Ministerio de Hacienda y Economía, Ministerio de Relaciones Exteriores, Ministerio de Interior y Policía, Ministerio de Salud Pública y Asistencia Social, Ministerio de Agricultura, Ministerio de Medio Ambiente y Recursos Naturales, Ministerio de Industria, Comercio y Mipymes, Dirección General de Migración, Dirección General de Aduanas, Cuerpo Especializado en Seguridad Fronteriza Terrestre —CESFRONT—, Dirección Nacional de Inteligencia —DNI—, Oficina Gubernamental de Tecnologías de la Información y Comunicación —OGTIC— e Instituto Dominicano de las Telecomunicaciones —INDOTEL—.

Los titulares podrán hacerse representar por funcionarios con competencia y capacidad suficientes para asumir compromisos institucionales dentro del ámbito autorizado.

**Párrafo I.-** En los asuntos relacionados con ciberseguridad, criptografía, infraestructura crítica de información o sistemas de alto interés para la seguridad nacional, la Dirección Nacional de Inteligencia garantizará la participación técnica de las dependencias u organismos especializados que correspondan conforme al marco jurídico vigente, incluidos el Centro Nacional de Ciberseguridad y el Instituto Criptográfico Nacional cuando resulte pertinente.

**Párrafo II.-** Podrán ser convocadas otras entidades públicas cuando la materia tratada corresponda a sus competencias.

**Párrafo III.-** La participación de órganos constitucionales autónomos o extrapoderes deberá realizarse respetando plenamente su autonomía e independencia y mediante los mecanismos jurídicos de coordinación correspondientes.

**Párrafo IV.-** La Comisión podrá escuchar con carácter consultivo a gobiernos locales fronterizos, universidades, centros de investigación, organizaciones productivas, empresariales o comunitarias y especialistas, sin que dicha participación otorgue acceso a información reservada, clasificada, personal o protegida.

### **Artículo 13.- Funciones de la Comisión.**

Corresponderá a la Comisión coordinar la ejecución general de la Política Nacional, conocer y dar seguimiento al Plan Maestro de Frontera Inteligente, promover la interoperabilidad entre las instituciones, identificar duplicidades tecnológicas, establecer prioridades estratégicas y evaluar los resultados generales de SIGFRO-RD.

La Comisión coordinará igualmente la elaboración de protocolos interinstitucionales, promoverá estándares comunes, conocerá los principales riesgos operacionales y tecnológicos y formulará recomendaciones para mejorar la continuidad, seguridad, eficiencia e integridad del sistema.

La Comisión presentará anualmente al Poder Ejecutivo un informe consolidado sobre los avances, resultados, dificultades, inversiones principales y recomendaciones de la Política Nacional.

**Párrafo I.-** Las prioridades identificadas por la Comisión en materia presupuestaria o de inversión pública deberán someterse a los procedimientos legalmente establecidos para planificación, evaluación, priorización, presupuesto y ejecución.

**Párrafo II.-** La Comisión no podrá ordenar la entrega de información cuyo acceso, utilización o divulgación esté limitado por la Constitución, una ley, una clasificación legítima o un régimen especial de protección.

#### **Artículo 14.- Secretaría Técnica Interinstitucional.**

La Comisión contará con una Secretaría Técnica Interinstitucional coordinada administrativamente por el Ministerio de la Presidencia y sustentada en las capacidades existentes de las instituciones participantes.

OGTIC coordinará los aspectos relativos a arquitectura digital gubernamental, interoperabilidad, estándares tecnológicos y servicios digitales compartidos. El Ministerio de Defensa coordinará los requerimientos operacionales vinculados con seguridad, vigilancia y continuidad de las operaciones fronterizas.

La Dirección Nacional de Inteligencia, en coordinación con los organismos y dependencias nacionales competentes en ciberseguridad y criptografía, ejercerá las funciones que le correspondan conforme a la Ley núm. 1-26, el Decreto núm. 612-24 y las demás disposiciones vigentes.

**Párrafo I.-** La Secretaría Técnica no constituirá una nueva entidad o dependencia con personalidad jurídica, patrimonio o nómina independiente.

**Párrafo II.-** Le corresponderá preparar los documentos técnicos de la Comisión, dar seguimiento a sus acuerdos, coordinar las mesas técnicas, mantener actualizada la arquitectura general de SIGFRO-RD y consolidar la información necesaria para su seguimiento y evaluación.

**Párrafo III.-** La coordinación prevista en este artículo no implicará transferencia o subordinación de las competencias legalmente atribuidas a las instituciones participantes.

#### **Artículo 15.- Responsabilidad institucional y protocolos de coordinación.**

Cada institución participante conservará la responsabilidad sobre los procesos, sistemas, datos, funcionarios e infraestructuras que se encuentren bajo su competencia.

Las operaciones en las que intervengan varias instituciones deberán regularse mediante protocolos que identifiquen claramente la autoridad funcional, los mecanismos de coordinación, la información susceptible de intercambio, los niveles de acceso, la respuesta ante contingencias y las responsabilidades de cada organismo.

Los protocolos no podrán modificar competencias establecidas por ley ni utilizarse para crear potestades, restricciones de derechos, sanciones o categorías jurídicas que requieran reserva legal.

## **CAPÍTULO IV**

### **PLANIFICACIÓN, INTEGRACIÓN Y CICLO DE VIDA TECNOLÓGICO**

#### **Artículo 16.- Plan Maestro de Frontera Inteligente.**

La implementación de la presente ley se desarrollará conforme a un Plan Maestro de Frontera Inteligente, de naturaleza plurianual, que constituirá el principal instrumento técnico de planificación de SIGFRO-RD.

El Plan deberá partir de un diagnóstico de las capacidades existentes y establecer la arquitectura tecnológica, prioridades territoriales, proyectos, responsabilidades institucionales, integraciones requeridas, necesidades de infraestructura, ciberseguridad, capacitación, inversión, mantenimiento, reposición e indicadores de resultado.

Su elaboración será coordinada por la Secretaría Técnica Interinstitucional y sometida a conocimiento de la Comisión.

**Párrafo I.-** La aprobación del Plan Maestro no sustituirá los procedimientos legalmente establecidos en materia de inversión pública, presupuesto, contrataciones, permisos ambientales, telecomunicaciones, aviación, construcción o cualquier otra autorización sectorial.

**Párrafo II.-** El Plan será objeto de revisión integral al menos cada cuatro años y podrá actualizarse cuando existan cambios sustanciales en los riesgos, la legislación, la infraestructura o la tecnología.

**Párrafo III.-** Las partes cuya divulgación pueda comprometer la seguridad nacional, capacidades operacionales, infraestructura crítica o vulnerabilidades tecnológicas estarán sometidas al régimen de protección que establezca el ordenamiento jurídico.

### **Artículo 17.- Integración prioritaria de capacidades existentes.**

Antes de autorizar el desarrollo o adquisición de una nueva solución destinada a SIGFRO-RD deberá determinarse si la necesidad puede ser satisfecha mediante la integración, ampliación o reutilización de sistemas estatales existentes.

La incorporación de nuevas tecnologías deberá estar sustentada en una necesidad comprobada y acompañarse de una evaluación sobre interoperabilidad, seguridad, costo total de propiedad, mantenimiento, vida útil, continuidad operacional y compatibilidad con la arquitectura general.

Las adquisiciones y desarrollos deberán cumplir la legislación vigente sobre contrataciones públicas, inversión, presupuesto y autorizaciones de tecnologías de la información, sin perjuicio de los regímenes especiales legalmente aplicables.

**Párrafo.-** Los contratos relacionados con componentes críticos deberán procurar portabilidad de la información, interoperabilidad, documentación técnica suficiente y mecanismos razonables que reduzcan dependencias innecesarias de un único proveedor.

### **Artículo 18.- Inventario Nacional de Infraestructura y Sistemas Fronterizos.**

Se establece el Inventario Nacional de Infraestructura y Sistemas Fronterizos —INISF—, como registro técnico de los sistemas, equipos e infraestructuras que formen parte o presten servicios esenciales a SIGFRO-RD.

El Inventario permitirá conocer la institución responsable, ubicación cuando corresponda, estado operacional, criticidad, mantenimiento, vida útil y necesidades de actualización o reposición de cada activo.

Su administración técnica corresponderá a la Secretaría Técnica Interinstitucional, sin modificar la propiedad, custodia, registro patrimonial ni responsabilidad institucional sobre los bienes.

**Párrafo I.-** Las instituciones estarán obligadas a mantener actualizada la información relativa a los activos bajo su responsabilidad.

**Párrafo II.-** La información cuya divulgación revele ubicación de equipos sensibles, arquitectura de redes, vulnerabilidades, configuraciones de seguridad o capacidades operacionales no tendrá carácter público por el solo hecho de encontrarse registrada en el Inventario.

**Párrafo III.-** Podrán publicarse estadísticas agregadas sobre cobertura, disponibilidad, inversión y mantenimiento cuando ello no comprometa la seguridad.

### **Artículo 19.- Operación, mantenimiento y reposición.**

Todo proyecto tecnológico incorporado a SIGFRO-RD deberá identificar desde su planificación los recursos y responsables necesarios para su operación, mantenimiento, actualización y eventual reposición.

La adquisición de un activo no podrá considerarse completa, para fines de planificación del sistema, sin considerar razonablemente su costo de operación durante el ciclo de vida.

Los equipos o sistemas que pierdan soporte de seguridad, presenten obsolescencia incompatible con las funciones requeridas o generen riesgos desproporcionados deberán incorporarse a programas de actualización o sustitución.

**Párrafo.-** Las instituciones deberán procurar capacidad técnica nacional para el mantenimiento ordinario de los componentes del sistema y transferencia de conocimientos cuando resulte razonablemente posible.

## **CAPÍTULO V**

### **GESTIÓN DIGITAL Y TRAZABILIDAD DEL EVENTO FRONTERIZO**

#### **Artículo 20.- Identificador Único de Evento Fronterizo.**

Se establece el Identificador Único de Evento Fronterizo —IUEF—, como código electrónico destinado a identificar y correlacionar las actuaciones asociadas a un mismo evento dentro de SIGFRO-RD.

El IUEF permitirá vincular técnicamente actuaciones realizadas por diferentes instituciones sin sustituir los números de expediente, declaración, investigación, acta, caso o registro utilizados por cada autoridad conforme a su legislación sectorial.

**Párrafo I.-** El IUEF será único, no reutilizable y susceptible de trazabilidad.

**Párrafo II.-** La asignación de un IUEF no constituirá por sí misma alerta migratoria, orden de arresto, autorización de entrada o salida, declaración aduanera, antecedente penal, decisión sancionadora ni prueba concluyente de una infracción.

#### **Artículo 21.- Expediente Digital del Evento Fronterizo.**

Los eventos registrados en SIGFRO-RD podrán generar un Expediente Digital del Evento Fronterizo —EDEF—, destinado a concentrar cronológicamente la información necesaria para reconstruir las actuaciones relacionadas con el evento.

El expediente podrá incorporar, conforme a los niveles de acceso correspondientes, información sobre el origen del evento, fecha, lugar, funcionarios intervinientes, consultas

realizadas, alertas, verificaciones, evidencias técnicas, actuaciones, decisiones y resultado final.

**Párrafo I.-** El EDEF tendrá naturaleza de registro operacional interinstitucional y no sustituirá el expediente administrativo, migratorio, aduanero, disciplinario, penal o judicial cuya formación sea requerida por legislación especial.

**Párrafo II.-** La inclusión de información dentro del EDEF no modificará su titularidad institucional, clasificación, régimen de protección ni período de conservación.

#### **Artículo 22.- Apertura y autoridad funcional del evento.**

Todo evento que requiera intervención institucional deberá quedar asociado a la autoridad que posea competencia legal principal respecto de la materia.

Cuando intervengan varias instituciones, SIGFRO-RD deberá permitir identificar la autoridad funcional principal y las instituciones que participen de manera complementaria.

La clasificación tecnológica de un evento tendrá carácter instrumental y no podrá alterar las competencias previstas por el ordenamiento jurídico.

**Párrafo.-** Una alerta automatizada podrá originar una verificación o remisión a la autoridad competente, pero no sustituirá el procedimiento ni la decisión que legalmente corresponda.

#### **Artículo 23.- Cierre, reapertura y correlación de eventos.**

El evento será cerrado cuando la autoridad funcional determine que la actuación operacional correspondiente ha concluido o haya sido transferida formalmente a otro procedimiento.

El cierre deberá dejar constancia del resultado y de la autoridad que lo dispuso.

Un evento cerrado podrá ser consultado por usuarios autorizados y reabierto cuando surjan nuevos elementos que lo justifiquen. Toda reapertura será trazable.

Cuando posteriormente se determine que dos o más eventos forman parte de una misma secuencia operacional, SIGFRO-RD podrá relacionarlos sin eliminar sus identificadores originales.

#### **Artículo 24.- Integridad y utilización de los registros digitales.**

Los registros generados por SIGFRO-RD deberán preservar, en la medida técnica aplicable, la identificación de su origen, fecha, hora, integridad y modificaciones.

Su utilización en procedimientos administrativos, disciplinarios, penales o judiciales estará sometida a las reglas de autenticidad, integridad, admisibilidad, cadena de custodia y valoración que establezca el ordenamiento jurídico.

La existencia de un registro tecnológico no sustituirá la obligación de motivar los actos administrativos ni las garantías de debido procedimiento.

**Párrafo.-** Cuando una imagen, video, lectura de sensor, registro electrónico u otro elemento deba extraerse para fines probatorios, deberá conservarse la vinculación con su fuente original y aplicarse los procedimientos de preservación que correspondan.

## **CAPÍTULO VI**

### **IDENTIDAD DIGITAL, CONTROL DE ACCESO Y AUDITORÍA DE USUARIOS**

#### **Artículo 25.- Identidad digital individual.**

Toda persona autorizada para operar directamente en SIGFRO-RD deberá disponer de una identidad digital individual, verificable e intransferible, vinculada con la institución y función correspondiente.

Queda prohibido el uso ordinario de cuentas compartidas o genéricas que impidan determinar quién realizó una actuación.

Cada institución será responsable de activar, modificar, suspender y revocar oportunamente las credenciales de su personal.

**Párrafo.-** Los contratistas, proveedores o técnicos externos que excepcionalmente necesiten acceso utilizarán credenciales individualizadas, temporales y limitadas a la finalidad autorizada.

#### **Artículo 26.- Principio de mínimo privilegio.**

El acceso a SIGFRO-RD se otorgará atendiendo a la competencia, función, necesidad y finalidad del usuario.

Ningún servidor público tendrá derecho a consultar toda la información disponible únicamente por razón de su rango, jerarquía o pertenencia a una institución participante.

Cuando para cumplir una función resulte suficiente que el sistema responda si una condición se encuentra validada, deberá privilegiarse esa respuesta sobre la exposición completa del expediente o base de datos.

Los permisos deberán revisarse periódicamente y siempre que cambien las responsabilidades del usuario.

### **Artículo 27.- Autenticación reforzada.**

Los sistemas críticos utilizarán mecanismos de autenticación proporcionales al riesgo y sensibilidad de la información.

Los accesos privilegiados, remotos y aquellos que determine la normativa técnica deberán utilizar autenticación multifactor u otro mecanismo de seguridad equivalente.

Los sistemas deberán impedir el uso permanente de credenciales predeterminadas por fabricantes o proveedores.

**Párrafo.-** Podrá establecerse acceso excepcional de emergencia cuando resulte indispensable para proteger personas, seguridad nacional, infraestructura crítica o continuidad operacional. Ese acceso deberá ser individual, limitado, registrado y sometido posteriormente a revisión.

### **Artículo 28.- Registro obligatorio de consultas y actuaciones.**

Las consultas y actuaciones relevantes efectuadas mediante SIGFRO-RD deberán producir automáticamente registros de auditoría suficientes para identificar al usuario, momento, sistema utilizado y naturaleza de la actuación.

Cuando la operación lo requiera, deberá quedar vinculada también al evento o finalidad que justifique la consulta.

Los registros estarán protegidos frente a alteración o eliminación no autorizada y ningún usuario podrá borrar los correspondientes a sus propias actuaciones.

Los administradores de sistemas estarán sujetos a un nivel de trazabilidad igual o superior al aplicado a los usuarios ordinarios.

### **Artículo 29.- Corrección y modificación de registros.**

Cuando se detecte un error en información cuya administración corresponda a una institución fuente, la corrección deberá realizarse en el sistema oficial de esa institución y posteriormente reflejarse en SIGFRO-RD conforme al mecanismo de interoperabilidad correspondiente.

Las correcciones de registros generados directamente por SIGFRO-RD deberán conservar el historial necesario para conocer el contenido anterior, la modificación realizada, su autor, fecha y fundamento.

Los registros de auditoría no serán alterados para ocultar una actuación. Las rectificaciones producirán nuevos registros vinculados con el original.

### **Artículo 30.- Supervisión de accesos privilegiados y de terceros.**

Los accesos con facultades administrativas, de mantenimiento o configuración estarán sometidos a controles reforzados.

El acceso remoto de proveedores o terceros requerirá autorización institucional, período definido, identificación individual y registro de las actuaciones realizadas.

Los mecanismos técnicos deberán procurar que ningún proveedor conserve accesos ocultos, permanentes o innecesarios a sistemas críticos una vez finalizada la actividad autorizada.

Las instituciones deberán revisar periódicamente las cuentas privilegiadas y eliminar aquellas que ya no resulten necesarias.

## **CAPÍTULO VII**

### **INTEROPERABILIDAD Y GOBERNANZA DE LOS DATOS**

#### **Artículo 31.- Arquitectura federada e institución fuente.**

SIGFRO-RD operará preferentemente mediante una arquitectura federada en la que cada institución conserve la administración y responsabilidad sobre los datos que legalmente le correspondan.

La interoperabilidad no implicará transferir o copiar indiscriminadamente bases institucionales completas cuando la finalidad pueda cumplirse mediante una consulta segura a la fuente oficial.

La institución que produzca o administre legítimamente un dato será considerada, para los fines de SIGFRO-RD, su institución fuente y conservará la responsabilidad principal sobre su actualización, corrección y calidad.

#### **Artículo 32.- Intercambio de información y minimización.**

El intercambio de información mediante SIGFRO-RD deberá tener una finalidad legítima y encontrarse vinculado con las competencias de las instituciones participantes.

Solo podrá intercambiarse la información necesaria y pertinente para la finalidad correspondiente.

Cuando la operación pueda resolverse mediante una respuesta de validación, confirmación, coincidencia o existencia de una alerta, deberá evitarse proporcionar información adicional que no resulte necesaria.

**Párrafo.-** La capacidad técnica de consultar un dato no constituirá por sí misma autorización jurídica para hacerlo.

### **Artículo 33.- Calidad, corrección y consistencia de los datos.**

Las instituciones deberán adoptar medidas razonables para procurar que los datos utilizados mediante SIGFRO-RD sean exactos, actualizados, pertinentes y consistentes con sus fuentes oficiales.

Cuando SIGFRO-RD detecte inconsistencias podrá remitirlas a la institución fuente para revisión, sin modificar unilateralmente sus registros.

Los estándares comunes necesarios para que conceptos, estados, categorías e identificadores tengan significado equivalente entre instituciones serán establecidos conforme a las normas gubernamentales de interoperabilidad.

**Párrafo.-** Una inconsistencia tecnológica o ausencia de respuesta de otro sistema no podrá interpretarse automáticamente como confirmación positiva de una condición.

### **Artículo 34.- Condiciones jurídicas de interoperabilidad.**

Las integraciones deberán apoyarse en la Constitución, las leyes, reglamentos y normas técnicas aplicables. Cuando sea necesario precisar responsabilidades, finalidades, categorías de información, niveles de acceso, conservación o seguridad, las instituciones celebrarán los convenios o protocolos correspondientes.

Estos instrumentos no podrán autorizar intercambios prohibidos por ley, ampliar competencias institucionales ni disminuir garantías constitucionales.

Las bases o sistemas sometidos a regímenes especiales de defensa, inteligencia, investigación penal, secreto legal o seguridad nacional conservarán las limitaciones y controles que les correspondan.

### **Artículo 35.- Seguridad, monitoreo y responsabilidad en el intercambio.**

Toda interoperabilidad deberá incorporar mecanismos que permitan identificar la institución solicitante, la fuente consultada, el momento de la operación y el resultado técnico de la transacción.

Las instituciones deberán monitorear el uso de sus servicios de interoperabilidad y podrán suspender preventivamente una integración cuando exista un incidente grave, compromiso de credenciales, riesgo cibernético significativo o utilización manifiestamente incompatible con las finalidades autorizadas.

La suspensión deberá comunicarse a las instituciones afectadas y documentarse, procurando restablecer el servicio cuando desaparezca la causa que la originó.

**Párrafo.-** Cuando la interrupción pueda afectar funciones esenciales de seguridad o control fronterizo, deberán activarse los mecanismos de contingencia previstos en el Plan Maestro y en los protocolos correspondientes.

## **CAPÍTULO VIII**

### **IDENTIFICACIÓN BIOMÉTRICA Y CONTROL MIGRATORIO**

#### **Artículo 36.- Finalidad de la identificación biométrica.**

La utilización de datos biométricos en el marco de SIGFRO-RD tendrá como finalidad contribuir a la verificación o identificación confiable de las personas sometidas legítimamente a procedimientos de control migratorio o fronterizo.

En materia migratoria, su utilización se realizará bajo las competencias de la Dirección General de Migración. Otras autoridades únicamente podrán tratar información biométrica cuando una disposición jurídica les reconozca dicha competencia y exclusivamente para la finalidad legalmente autorizada.

La biometría constituirá un instrumento auxiliar de identificación y seguridad y no sustituirá los documentos, autorizaciones, categorías migratorias ni procedimientos establecidos por la legislación vigente.

**Párrafo.-** Ningún registro, credencial o constancia tecnológica creada al amparo de esta ley podrá conferir por sí misma condición migratoria regular, autorización de permanencia o derecho de entrada o salida cuando dicha condición o autorización corresponda ser determinada por la autoridad migratoria competente.

#### **Artículo 37.- Captura y tratamiento de datos biométricos.**

La captura y tratamiento de datos biométricos deberá realizarse únicamente cuando exista fundamento jurídico, finalidad determinada y competencia institucional para ello.

Los sistemas deberán incorporar medidas reforzadas de seguridad, control de acceso, trazabilidad y protección frente a copia, alteración o utilización no autorizada.

Cuando para una consulta interinstitucional resulte suficiente conocer el resultado de una verificación biométrica, deberá privilegiarse la transmisión de dicho resultado sobre la entrega del archivo biométrico original.

**Párrafo.-** El tratamiento de datos biométricos deberá observar el artículo 44 de la Constitución, la Ley núm. 172-13 y los regímenes especiales que resulten aplicables.

### **Artículo 38.- Verificación secundaria.**

Cuando una comprobación biométrica resulte inconclusa, presente inconsistencias o no alcance los niveles técnicos de confiabilidad establecidos, la persona será remitida al procedimiento de verificación secundaria correspondiente.

La ausencia de coincidencia biométrica o el fallo técnico de un dispositivo no constituirá por sí mismo prueba de irregularidad migratoria, falsedad de identidad ni comisión de una infracción.

La autoridad competente deberá considerar la documentación disponible y las demás verificaciones previstas por el ordenamiento jurídico antes de adoptar una decisión.

### **Artículo 39.- Control migratorio en mercados y regímenes fronterizos.**

Los mecanismos tecnológicos aplicados a mercados binacionales, actividades comerciales fronterizas o modalidades de tránsito recurrente deberán operar exclusivamente dentro de los regímenes jurídicamente reconocidos.

La Dirección General de Migración podrá utilizar registros biométricos, controles electrónicos y mecanismos de validación para facilitar la identificación y registro de las personas autorizadas a participar en dichas actividades.

Estos mecanismos no crearán nuevas categorías migratorias ni podrán utilizarse para otorgar derechos de permanencia, residencia, trabajo o circulación distintos de los establecidos por la legislación vigente.

### **Artículo 40.- Decisión migratoria y control humano.**

Toda decisión migratoria que produzca efectos jurídicos relevantes sobre una persona será adoptada por la autoridad competente conforme a la legislación migratoria.

Una coincidencia biométrica, alerta automática, reconocimiento facial, recomendación algorítmica o clasificación de riesgo podrá justificar una revisión adicional, pero no constituirá por sí sola fundamento suficiente para adoptar una decisión definitiva de rechazo, deportación, detención u otra medida restrictiva de derechos.

La actuación deberá quedar vinculada al registro correspondiente y ser susceptible de revisión conforme a los procedimientos aplicables.

## CAPÍTULO IX

### IDENTIFICACIÓN Y CONTROL VEHICULAR FRONTERIZO

#### **Artículo 41.- Sistema de identificación vehicular fronteriza.**

El control tecnológico de vehículos que participen en operaciones fronterizas deberá integrarse prioritariamente con las plataformas y programas oficiales administrados por la Dirección General de Aduanas, incluido el sistema de Identificación Vehicular Fronteriza — IVF-RD— o aquel que legalmente lo sustituya.

SIGFRO-RD no desarrollará un sistema paralelo cuando las funcionalidades requeridas puedan obtenerse mediante integración con los sistemas oficiales existentes.

#### **Artículo 42.- Identidad electrónica del vehículo.**

La identificación tecnológica de un vehículo podrá relacionar la matrícula, número de identificación vehicular o chasis, características físicas, propietario o responsable registrado, imágenes y los dispositivos electrónicos de identificación autorizados por la autoridad competente.

La utilización de un identificador electrónico no constituirá por sí misma prueba de propiedad, autorización aduanera, autorización migratoria ni derecho de circulación.

Las divergencias entre los distintos elementos de identificación deberán generar verificación adicional.

#### **Artículo 43.- Lectura y registro automatizado.**

Los puntos fronterizos habilitados podrán utilizar sistemas de lectura automática de matrículas, identificación por radiofrecuencia, códigos seguros, imágenes u otras tecnologías legalmente autorizadas para registrar el movimiento de vehículos.

Las lecturas relevantes podrán quedar vinculadas al IUEF y a las operaciones migratorias, aduaneras, comerciales o de seguridad correspondientes.

La tecnología deberá configurarse para limitar la recopilación y utilización de la información a las finalidades legítimas establecidas por el ordenamiento jurídico.

#### **Artículo 44.- Vehículos extranjeros y regímenes temporales.**

Los vehículos extranjeros que ingresen al territorio nacional estarán sujetos a los regímenes aduaneros, migratorios, de tránsito y demás disposiciones legalmente aplicables.

Cuando corresponda, podrán recibir mecanismos electrónicos temporales de identificación destinados a relacionar el vehículo con su responsable, régimen autorizado, fecha de entrada y demás información necesaria para su control.

La identificación tecnológica no modificará las condiciones, plazos ni obligaciones del régimen jurídico bajo el cual haya sido admitido el vehículo.

**Artículo 45.- Inconsistencias y revisión vehicular.**

Cuando el sistema detecte inconsistencias relevantes entre matrícula, chasis, identificador electrónico, imágenes, documentación o historial de la operación, podrá generar una alerta para revisión por la autoridad competente.

La alerta no constituirá por sí misma determinación de fraude, contrabando, robo o cualquier otra infracción.

Toda inmovilización, retención, inspección adicional o medida equivalente deberá realizarse conforme a las competencias y procedimientos establecidos por la legislación aplicable.

## **CAPÍTULO X**

### **ADUANA INTELIGENTE Y TRAZABILIDAD DE MERCANCÍAS**

**Artículo 46.- Principio de integración aduanera.**

La tecnificación de los procedimientos aduaneros fronterizos se realizará bajo la autoridad de la Dirección General de Aduanas, conforme a la Ley núm. 168-21, su Reglamento General de Aplicación y las demás normas vigentes.

SIGFRO-RD funcionará como mecanismo complementario de interoperabilidad y trazabilidad y no sustituirá el sistema aduanero oficial ni las facultades de control, fiscalización, determinación, inspección o despacho atribuidas a la Dirección General de Aduanas.

**Artículo 47.- Información anticipada y gestión de riesgo.**

Cuando el régimen aduanero aplicable lo permita, la información relativa a la mercancía, transportista, vehículo, documentos y autorizaciones podrá ser recibida y procesada antes de la llegada física al punto fronterizo.

La Dirección General de Aduanas podrá utilizar dicha información para realizar análisis de riesgo y determinar los niveles de control correspondientes.

La gestión de riesgo deberá procurar simultáneamente fortalecer la fiscalización y facilitar las operaciones legítimas, evitando controles innecesariamente uniformes cuando sea posible aplicar procedimientos diferenciados.

#### **Artículo 48.- Trazabilidad de la operación aduanera.**

Las operaciones sujetas a control podrán vincular digitalmente la declaración aduanera, mercancía, transportista, conductor, vehículo, contenedor o remolque, inspecciones efectuadas, autorizaciones y resultado final del procedimiento.

La trazabilidad deberá permitir identificar las principales actuaciones realizadas durante el proceso y los funcionarios que hayan intervenido cuando corresponda.

El IUEF podrá utilizarse como referencia de correlación sin sustituir la declaración aduanera, el expediente o los identificadores propios de la Dirección General de Aduanas.

#### **Artículo 49.- Pesaje, inspección y dispositivos de seguridad.**

La Dirección General de Aduanas podrá integrar a sus procedimientos sistemas automáticos de pesaje, inspección no intrusiva, precintos electrónicos y demás tecnologías de control previstas o permitidas por la legislación vigente.

Los resultados obtenidos podrán incorporarse electrónicamente al registro de la operación, procurando reducir la introducción manual de información cuando el dispositivo utilizado pueda transmitirla directamente de manera segura.

Toda discrepancia significativa deberá ser evaluada conforme a los procedimientos aduaneros correspondientes.

#### **Artículo 50.- Coordinación con organismos de control especializado.**

Cuando una mercancía requiera intervención sanitaria, fitosanitaria, zoosanitaria, ambiental o de otra autoridad especializada, SIGFRO-RD podrá facilitar la coordinación y el intercambio de la información necesaria entre la Dirección General de Aduanas y el organismo competente.

La interoperabilidad no alterará la atribución legal de cada institución para emitir permisos, certificaciones, objeciones, retenciones o decisiones dentro de su respectiva materia.

Se procurará evitar la presentación repetida de información que ya obre válidamente en poder del Estado y pueda ser reutilizada conforme a la ley.

## CAPÍTULO XI

### VIGILANCIA ELECTRÓNICA Y RED INTEGRADA DE SENSORES FRONTERIZOS

#### **Artículo 51.- Red Integrada de Sensores Fronterizos.**

La vigilancia tecnológica de la frontera podrá apoyarse en una Red Integrada de Sensores Fronterizos —RISF—, compuesta por los dispositivos legalmente autorizados que permitan detectar, observar, localizar y verificar eventos relevantes para la seguridad y gestión fronteriza.

La Red formará parte de SIGFRO-RD y se integrará con los centros de mando y capacidades operacionales existentes, procurando aprovechar la infraestructura ya desplegada por el Estado.

#### **Artículo 52.- Finalidad, proporcionalidad y límites de la vigilancia.**

Los sistemas de vigilancia electrónica deberán orientarse exclusivamente a finalidades públicas legítimas vinculadas con seguridad fronteriza, protección territorial, control de puntos habilitados, protección de infraestructura y demás competencias previstas por el ordenamiento jurídico.

Su ubicación, alcance y utilización deberán guardar proporcionalidad con los riesgos que se pretendan gestionar.

La presente ley no autoriza la captación deliberada del interior de domicilios, la interceptación de comunicaciones privadas ni cualquier otra forma de vigilancia que, conforme a la Constitución y las leyes, requiera autorización judicial o procedimiento especial.

Cuando la infraestructura tecnológica se encuentre próxima a viviendas, comunidades o espacios privados deberán adoptarse medidas razonables para reducir la captación innecesaria de información ajena a la finalidad legítima perseguida.

#### **Artículo 53.- Fusión y verificación de alertas.**

SIGFRO-RD podrá correlacionar señales provenientes de diferentes sensores con el propósito de mejorar la confiabilidad de las alertas.

Cuando las condiciones operacionales lo permitan, los eventos generados automáticamente podrán ser confirmados mediante otra fuente tecnológica o por personal autorizado antes de disponer una respuesta que implique movilización significativa de recursos o afectación de derechos.

Lo anterior no impedirá la actuación inmediata cuando la naturaleza del evento razonablemente indique peligro, emergencia o necesidad urgente de intervención.

#### **Artículo 54.- Disponibilidad y mantenimiento.**

Los sensores y equipos de vigilancia deberán estar incorporados al Inventario Nacional de Infraestructura y Sistemas Fronterizos y sometidos a mantenimiento preventivo y correctivo conforme a su nivel de criticidad.

Los equipos críticos deberán, cuando técnicamente resulte posible, disponer de mecanismos que permitan detectar pérdida de comunicación, interrupción de energía, manipulación, falla o degradación significativa.

Las indisponibilidades relevantes deberán quedar registradas y ser gestionadas conforme a los protocolos de continuidad operacional.

#### **Artículo 55.- Conservación y acceso a imágenes y registros.**

Las imágenes, grabaciones y demás información producida por la vigilancia electrónica estarán sujetas a períodos de conservación diferenciados según su finalidad, naturaleza, existencia de incidentes, investigaciones abiertas y demás exigencias legales.

El acceso deberá encontrarse restringido por función y quedar sujeto a trazabilidad.

La extracción de registros para investigaciones o procesos deberá preservar razonablemente su integridad, origen y cadena de custodia conforme al ordenamiento jurídico.

## **CAPÍTULO XII**

### **SISTEMA DE AERONAVES NO TRIPULADAS PARA LA GESTIÓN FRONTERIZA**

#### **Artículo 56.- Sistema de aeronaves no tripuladas.**

Las instituciones competentes podrán integrar aeronaves no tripuladas a las funciones de vigilancia, reconocimiento, verificación, inspección de infraestructura, protección ambiental, búsqueda, rescate y demás actividades legítimamente vinculadas con la gestión fronteriza.

Estas capacidades se coordinarán dentro de SIGFRO-RD y con las estructuras de mando existentes, evitando la creación injustificada de flotas o plataformas incompatibles entre instituciones.

**Párrafo.-** La utilización de aeronaves no tripuladas no autorizará la vigilancia deliberada del interior de domicilios, la interceptación de comunicaciones privadas ni otras actuaciones sometidas constitucional o legalmente a autorización judicial. Las rutas, sistemas de

geocercado y procedimientos operacionales deberán además adoptar medidas destinadas a impedir incursiones no autorizadas en el espacio aéreo de otro Estado.

**Artículo 57.- Régimen aeronáutico y seguridad operacional.**

Las operaciones de aeronaves no tripuladas deberán cumplir la legislación aeronáutica dominicana y los Reglamentos Aeronáuticos Dominicanos aplicables, así como las autorizaciones y requisitos del Instituto Dominicano de Aviación Civil cuando correspondan.

Lo anterior se aplicará sin perjuicio de los regímenes especiales que el ordenamiento jurídico reconozca para operaciones militares, de seguridad o de Estado.

Las instituciones deberán coordinar sus operaciones de manera que no comprometan la seguridad de la aviación civil ni produzcan incursiones no autorizadas en espacio aéreo extranjero.

**Artículo 58.- Operaciones automatizadas.**

Las aeronaves no tripuladas podrán ejecutar misiones programadas o parcialmente automatizadas cuando la tecnología, la regulación aeronáutica y las condiciones de seguridad lo permitan.

Toda misión deberá conservar trazabilidad suficiente respecto de la aeronave utilizada, unidad responsable, período de operación y datos producidos.

Los sistemas automatizados podrán detectar y seguir objetos o eventos, pero las decisiones operacionales que impliquen coerción permanecerán bajo control de la autoridad competente.

**Artículo 59.- Prohibición de empleo autónomo de fuerza.**

Las aeronaves no tripuladas utilizadas en virtud de esta ley tendrán funciones de observación, reconocimiento, verificación y apoyo operacional.

No podrán ser configuradas para decidir de manera autónoma el empleo de fuerza contra personas.

La presente ley no constituye autorización para crear o emplear sistemas autónomos de armas ni modifica las reglas constitucionales, legales y operacionales aplicables al uso legítimo de la fuerza por los órganos del Estado.

**Artículo 60.- Seguridad tecnológica y control de las aeronaves.**

Las aeronaves no tripuladas, estaciones de control y sistemas asociados deberán estar sometidos a medidas apropiadas de ciberseguridad, mantenimiento, control de software, protección de comunicaciones y gestión de accesos.

Las adquisiciones deberán considerar la capacidad del Estado para administrar los datos producidos, controlar actualizaciones, mantener los equipos y limitar accesos remotos no autorizados.

Cuando se utilicen tecnologías destinadas a detectar o contrarrestar aeronaves no tripuladas no autorizadas, su operación deberá ajustarse a las competencias legales y al régimen de telecomunicaciones, aviación, defensa y seguridad que resulte aplicable.

## **CAPÍTULO XIII**

### **INTELIGENCIA ARTIFICIAL, ANÁLISIS DE RIESGO Y SISTEMAS AUTOMATIZADOS**

#### **Artículo 61.- Utilización de inteligencia artificial y sistemas automatizados.**

SIGFRO-RD podrá utilizar herramientas de inteligencia artificial, analítica avanzada, modelos estadísticos y otros sistemas automatizados para apoyar la detección de anomalías, clasificación de eventos, análisis de riesgo, gestión de recursos, vigilancia tecnológica, mantenimiento predictivo y demás funciones compatibles con la presente ley.

Su utilización deberá ajustarse a la Constitución, la Estrategia Nacional de Inteligencia Artificial vigente, las normas de protección de datos, los principios de legalidad, necesidad y proporcionalidad y las demás disposiciones que regulen la transformación digital del Estado.

Los sistemas automatizados tendrán naturaleza instrumental y no adquirirán competencia administrativa propia.

#### **Artículo 62.- Análisis y clasificación de riesgo.**

Las instituciones competentes podrán utilizar mecanismos automatizados para clasificar el nivel de riesgo de operaciones, eventos, vehículos, mercancías o situaciones fronterizas cuando dicha clasificación se encuentre vinculada con una finalidad legítima y con las competencias legales de la institución correspondiente.

Los criterios utilizados deberán guardar relación objetiva con el riesgo evaluado, ser susceptibles de revisión y evitar variables carentes de fundamento jurídico o técnico.

Una clasificación de riesgo podrá determinar la necesidad de verificación adicional, priorización de recursos o inspección conforme al régimen sectorial aplicable, pero no constituirá por sí misma determinación de responsabilidad o comisión de una infracción.

### **Artículo 63.- Decisiones de alto impacto y revisión humana.**

Ninguna decisión estatal que pueda producir efectos jurídicos o materiales significativos sobre una persona podrá fundamentarse exclusivamente en el resultado de un sistema automatizado.

Las decisiones que puedan conducir a rechazo migratorio, deportación, detención, incautación, sanción o restricciones equivalentes deberán ser adoptadas por la autoridad legalmente competente, con posibilidad real de examinar la información utilizada, ordenar verificaciones adicionales y apartarse de la recomendación tecnológica cuando corresponda.

La intervención humana deberá ser efectiva y no limitarse a confirmar automáticamente la recomendación del sistema.

### **Artículo 64.- Registro y evaluación de modelos de alto impacto.**

Los modelos de inteligencia artificial o análisis automatizado utilizados de manera permanente en funciones de alto impacto deberán encontrarse documentados dentro de un registro técnico administrado conforme a las normas gubernamentales aplicables.

La documentación deberá permitir identificar, al menos, su finalidad, institución responsable, versión, proveedor o desarrollador, fecha de puesta en operación y resultados de las evaluaciones efectuadas.

Antes de su utilización en operaciones de alto impacto deberán someterse a pruebas razonables de precisión, robustez, seguridad, falsos positivos, falsos negativos y posibles sesgos. Estas evaluaciones deberán repetirse periódicamente y cuando se produzcan cambios sustanciales del modelo.

**Párrafo.-** La información cuya divulgación pueda permitir evadir controles, comprometer sistemas de seguridad o revelar información protegida no tendrá carácter público por el solo hecho de formar parte del registro.

### **Artículo 65.- No discriminación, explicabilidad y corrección.**

Los sistemas automatizados no podrán considerar irregular a una persona exclusivamente por su raza, color, origen étnico real o percibido, religión, opinión política, apariencia física u otra condición protegida por la Constitución.

Cuando la nacionalidad, condición migratoria u otra circunstancia personal resulte jurídicamente relevante para una actuación fronteriza, deberá determinarse mediante documentos, registros oficiales y procedimientos legalmente establecidos, y no mediante inferencias basadas exclusivamente en apariencia, idioma o acento.

Cuando una recomendación automatizada origine una intervención relevante, la autoridad deberá disponer, en la medida técnicamente posible, de información suficiente para conocer los factores principales que justificaron la alerta.

Los errores confirmados, falsos positivos y decisiones humanas que razonablemente contradigan al modelo deberán registrarse y utilizarse para su evaluación y mejora.

## **CAPÍTULO XIV**

### **CIBERSEGURIDAD, RESILIENCIA Y CONTINUIDAD OPERACIONAL**

#### **Artículo 66.- Seguridad de la infraestructura digital fronteriza.**

Los sistemas, redes, plataformas, sensores, centros de procesamiento y demás componentes críticos de SIGFRO-RD deberán diseñarse, operar y mantenerse conforme a principios de seguridad por diseño, defensa en profundidad, mínimo privilegio, segmentación, resiliencia y mejora continua.

La gestión de ciberseguridad deberá ajustarse a la legislación y estrategia nacional vigentes, a la Ley núm. 1-26, al Decreto núm. 612-24 y a las disposiciones dictadas por las autoridades nacionales competentes.

En el ámbito técnico gubernamental deberán observarse, según corresponda, la NORTIC A7 sobre Administración de la Seguridad de la Información, la NORTIC A8 sobre Ciberseguridad y las normas que las modifiquen o sustituyan.

La clasificación de componentes de SIGFRO-RD como infraestructura crítica de información se efectuará conforme a los criterios, procedimientos y autoridades establecidos en el marco nacional correspondiente.

#### **Artículo 67.- Gestión de riesgos y segmentación.**

Cada institución participante deberá identificar y gestionar los riesgos de ciberseguridad de los componentes de SIGFRO-RD bajo su responsabilidad.

La arquitectura deberá procurar que el compromiso de un dispositivo o segmento no permita automáticamente acceder a sistemas de mayor sensibilidad. Las redes administrativas, operacionales, de vigilancia, biométricas y demás entornos críticos deberán mantener los niveles de separación que determinen el riesgo y las normas técnicas vigentes.

Los accesos administrativos, remotos y de proveedores estarán sometidos a controles reforzados y a trazabilidad.

#### **Artículo 68.- Incidentes de ciberseguridad.**

Las instituciones estarán obligadas a detectar, documentar y gestionar los incidentes de ciberseguridad que afecten o puedan afectar SIGFRO-RD y a notificarlos conforme a los procedimientos nacionales vigentes.

La respuesta deberá coordinarse con las autoridades y equipos nacionales competentes según la naturaleza y gravedad del incidente, sin perjuicio de las actuaciones que correspondan a los organismos de investigación y persecución penal cuando existan indicios de infracciones previstas por la Ley núm. 53-07 u otra legislación aplicable.

La notificación de un incidente no eximirá a la institución responsable de adoptar inmediatamente las medidas necesarias para contenerlo y preservar la continuidad de los servicios esenciales.

#### **Artículo 69.- Continuidad y recuperación.**

Los componentes críticos de SIGFRO-RD deberán disponer de planes de continuidad y recuperación proporcionales a su importancia operacional.

La planificación deberá prever fallos de energía, interrupciones de telecomunicaciones, indisponibilidad de sistemas, ataques cibernéticos, desastres naturales y demás situaciones capaces de afectar las operaciones fronterizas.

Cuando resulte técnicamente razonable, los puntos esenciales deberán disponer de medios alternativos de energía, comunicación, almacenamiento o procesamiento y de procedimientos que permitan operar temporalmente bajo condiciones degradadas.

La operación manual o de contingencia deberá quedar posteriormente registrada e integrada a los sistemas correspondientes tan pronto resulte posible.

#### **Artículo 70.- Seguridad de proveedores y cadena tecnológica.**

Las adquisiciones, contratos de mantenimiento, licencias y servicios tecnológicos destinados a SIGFRO-RD deberán incorporar requisitos de ciberseguridad proporcionales al nivel de riesgo.

Las instituciones deberán evaluar la capacidad de los proveedores para proteger la información, corregir vulnerabilidades, controlar accesos remotos, mantener los equipos y garantizar la continuidad y portabilidad de los servicios.

Ningún proveedor deberá utilizar datos producidos en el ejercicio de funciones públicas para finalidades distintas de las autorizadas ni conservar accesos permanentes innecesarios a infraestructura crítica.

Las obligaciones de seguridad deberán mantenerse durante toda la vigencia contractual y, cuando corresponda, durante el período posterior necesario para la devolución, migración o destrucción segura de la información.

## **CAPÍTULO XV**

### **INTEGRIDAD INSTITUCIONAL Y PREVENCIÓN DE ACTUACIONES IRREGULARES**

#### **Artículo 71.- Trazabilidad como mecanismo de integridad.**

SIGFRO-RD deberá utilizar la trazabilidad de las actuaciones como instrumento para fortalecer el control interno, la transparencia y la responsabilidad individual de los servidores públicos.

Las autorizaciones, anulaciones, modificaciones, excepciones y demás actuaciones de especial relevancia deberán permitir identificar al funcionario interviniente y conservar información suficiente para una revisión posterior.

La digitalización de un procedimiento no disminuirá las responsabilidades administrativas, disciplinarias, civiles o penales previstas por el ordenamiento jurídico.

#### **Artículo 72.- Segregación y doble control.**

Las instituciones deberán identificar aquellas operaciones en las que la concentración de facultades en una sola persona genere riesgos relevantes de fraude, corrupción, manipulación o conflicto de interés.

En tales casos podrán establecer mecanismos de segregación de funciones, asignación automatizada, revisión superior o doble autorización, procurando que la intensidad del control sea proporcional al riesgo.

La reasignación manual de un expediente o la excepción a un control automatizado deberá quedar registrada cuando la naturaleza del procedimiento lo justifique.

#### **Artículo 73.- Analítica de integridad.**

SIGFRO-RD podrá utilizar herramientas analíticas para identificar patrones administrativos anómalos, tales como utilización extraordinaria de excepciones, anulaciones recurrentes, accesos sin relación aparente con las funciones del usuario o concentraciones inusuales de operaciones.

La detección de una anomalía tendrá carácter preventivo y podrá dar lugar a revisión, auditoría o investigación conforme al procedimiento correspondiente.

Ningún patrón estadístico constituirá por sí solo prueba de corrupción, falta disciplinaria o responsabilidad penal.

**Artículo 74.- Contrataciones, proveedores y conflictos de interés.**

Las contrataciones relacionadas con SIGFRO-RD se regirán por la Ley núm. 47-25 de Contrataciones Públicas, su Reglamento de Aplicación y las disposiciones especiales que resulten válidamente aplicables a adquisiciones relacionadas con seguridad nacional.

Los procedimientos deberán procurar competencia, trazabilidad, seguridad de la información, sostenibilidad financiera y prevención de conflictos de interés.

La naturaleza sensible de determinados bienes o servicios no constituirá por sí sola fundamento para excluir los controles de contratación, fiscalización o rendición de cuentas establecidos por el ordenamiento jurídico.

**Párrafo.-** Cuando proceda legítimamente una modalidad especial o reserva de información por razones de seguridad nacional, deberá aplicarse exclusivamente en la medida prevista por la legislación vigente.

**Artículo 75.- Control interno y responsabilidad funcional.**

Las instituciones participantes deberán incorporar los componentes de SIGFRO-RD dentro de sus sistemas de control interno, gestión de riesgos y auditoría.

Los hallazgos que indiquen posibles faltas administrativas o disciplinarias deberán tramitarse conforme a la Ley núm. 41-08 de Función Pública, los regímenes especiales aplicables y las garantías del debido procedimiento.

Cuando los hechos puedan constituir infracción penal, deberán ser puestos en conocimiento de la autoridad competente conforme al ordenamiento jurídico.

La actuación de los órganos de control interno no sustituirá las atribuciones de la Contraloría General de la República, Cámara de Cuentas u otros órganos de fiscalización dentro de sus respectivas competencias.

## **CAPÍTULO XVI**

### **COMERCIO FRONTERIZO, CENTROS LOGÍSTICOS Y FACILITACIÓN**

**Artículo 76.- Principio de facilitación del comercio legítimo.**

La tecnificación fronteriza deberá procurar simultáneamente fortalecer los controles y facilitar el comercio lícito.

Los procedimientos deberán orientarse a reducir duplicidades, tiempos innecesarios y trámites repetitivos, aplicando gestión de riesgo, interoperabilidad y digitalización cuando ello resulte compatible con la legislación aduanera, tributaria, sanitaria y comercial.

La facilitación no implicará exención de controles, tributos, permisos o requisitos legalmente exigibles.

#### **Artículo 77.- Centros logísticos y puertos secos.**

Los proyectos de centros logísticos, instalaciones interiores de despacho y demás infraestructuras destinadas a organizar el comercio fronterizo deberán desarrollarse dentro de los regímenes jurídicos existentes, particularmente la Ley núm. 30-24 sobre Centros Logísticos, la Ley núm. 168-21 General de Aduanas y las demás disposiciones aplicables.

La presente ley no creará por sí misma un régimen aduanero, fiscal o de zona franca distinto de los establecidos en la legislación vigente.

La integración de estas instalaciones a SIGFRO-RD deberá permitir la trazabilidad de las operaciones sin alterar las competencias de Aduanas ni de los demás organismos de control.

#### **Artículo 78.- Digitalización de operaciones logísticas.**

Las instalaciones fronterizas podrán utilizar sistemas de pre-registro, programación de llegada, identificación electrónica, control de acceso, pesaje, almacenamiento y seguimiento de operaciones.

Cuando un dato válido ya se encuentre en poder de un órgano estatal y exista fundamento jurídico para su reutilización, deberá procurarse evitar que el operador tenga que presentarlo nuevamente ante otra institución.

La interoperabilidad deberá respetar las reglas de protección de datos, secreto fiscal, reserva comercial y demás limitaciones legalmente aplicables.

#### **Artículo 79.- Pequeños comerciantes y formalización progresiva.**

La modernización de la frontera deberá considerar mecanismos que faciliten la incorporación progresiva de pequeños comerciantes y operadores al comercio formal, sin crear mediante esta ley exenciones tributarias, aduaneras o migratorias no previstas en otras normas.

Los programas podrán apoyarse en registros simplificados, asistencia técnica, educación aduanera, medios digitales de pago y procedimientos simplificados que hayan sido previamente autorizados por las autoridades competentes.

Los mercados fronterizos podrán integrarse tecnológicamente a SIGFRO-RD cuando ello resulte necesario para mejorar seguridad, ordenamiento, identificación y trazabilidad.

## **Artículo 80.- Desarrollo económico fronterizo.**

La implementación de esta ley deberá coordinarse con el régimen establecido por la Ley núm. 12-21 sobre la Zona Especial de Desarrollo Integral Fronterizo y con las demás políticas nacionales dirigidas a inversión, empleo, infraestructura y desarrollo productivo de las provincias fronterizas.

Las inversiones tecnológicas y logísticas deberán procurar generar encadenamientos con productores, empresas, trabajadores y centros de formación de la región.

Los incentivos económicos que resulten aplicables serán exclusivamente aquellos establecidos conforme al ordenamiento jurídico correspondiente.

## **CAPÍTULO XVII**

### **BIOSEGURIDAD, CONTROL SANITARIO Y PROTECCIÓN AMBIENTAL**

#### **Artículo 81.- Componente integrado de bioseguridad fronteriza.**

SIGFRO-RD incorporará mecanismos de coordinación tecnológica destinados a apoyar la prevención y control de riesgos para la salud humana, la sanidad vegetal, la sanidad animal, la inocuidad de alimentos y los recursos naturales.

Las actuaciones corresponderán en todo momento a las autoridades que posean competencia legal en cada materia.

La interoperabilidad tendrá como finalidad facilitar alertas, verificaciones, inspecciones y trazabilidad, sin sustituir permisos, certificados, cuarentenas u otras decisiones sectoriales.

#### **Artículo 82.- Vigilancia sanitaria.**

El Ministerio de Salud Pública podrá integrar a SIGFRO-RD las alertas y procedimientos fronterizos necesarios para cumplir sus competencias conforme a la Ley General de Salud núm. 42-01 y demás disposiciones aplicables.

Cuando exista un riesgo sanitario que requiera intervención, el sistema podrá generar una remisión a la autoridad sanitaria competente y facilitar el intercambio de la información estrictamente necesaria.

La información clínica o sanitaria de carácter personal estará sometida a protección reforzada y no será accesible indiscriminadamente a funcionarios de seguridad, migración o aduanas.

### **Artículo 83.- Sanidad vegetal y animal.**

Las autoridades agropecuarias competentes podrán utilizar SIGFRO-RD para apoyar los controles cuarentenarios, fitosanitarios y zoonosanitarios aplicables a animales, plantas, productos, subproductos y otros artículos regulados.

Los permisos, certificaciones, retenciones, tratamientos, cuarentenas, prohibiciones o medidas equivalentes continuarán rigiéndose por la normativa agropecuaria correspondiente.

Cuando resulte posible, la plataforma deberá interoperar con los sistemas oficiales de autorización y con la Ventanilla Única de Comercio Exterior, evitando la creación de registros paralelos.

### **Artículo 84.- Trazabilidad de inspecciones y muestras.**

Cuando una operación fronteriza requiera inspección sanitaria, agropecuaria o toma de muestras, el resultado podrá vincularse al evento correspondiente en SIGFRO-RD.

La plataforma podrá registrar la mercancía u objeto inspeccionado, autoridad actuante, lugar, fecha, muestra obtenida, laboratorio competente y resultado, respetando las reglas técnicas y jurídicas aplicables.

Cuando el resultado produzca una medida restrictiva, esta deberá ser adoptada por la autoridad sectorial competente y conforme al procedimiento establecido.

### **Artículo 85.- Protección ambiental y monitoreo territorial.**

Las capacidades tecnológicas de SIGFRO-RD podrán apoyar al Ministerio de Medio Ambiente y Recursos Naturales en la detección y monitoreo de incendios, afectaciones de áreas protegidas, tala, extracción irregular de recursos, contaminación, daños a cuencas y otros eventos ambientales dentro de sus competencias.

La utilización de cámaras, drones, sensores o información geoespacial para fines ambientales no transferirá al personal de seguridad competencias sancionadoras o regulatorias propias de la autoridad ambiental.

Las nuevas infraestructuras construidas para la implementación de esta ley deberán cumplir las obligaciones de evaluación y autorización ambiental previstas por la Ley núm. 64-00 y sus normas complementarias cuando resulten aplicables.

## CAPÍTULO XVIII

### DESARROLLO ECONÓMICO, SOCIAL Y TERRITORIAL DE LA ZONA FRONTERIZA

#### **Artículo 86.- Integración de seguridad y desarrollo.**

La implementación de la Política Nacional de Gestión Integrada y Tecnificación Fronteriza deberá considerar la seguridad y el desarrollo económico y social de la zona fronteriza como componentes complementarios de una misma política de Estado.

Las inversiones en infraestructura de control, comunicaciones, logística y tecnología deberán procurar, cuando resulte compatible con su finalidad principal, contribuir al fortalecimiento de la actividad productiva, conectividad, capacitación técnica, empleo y prestación de servicios en las comunidades fronterizas.

La ejecución de este capítulo deberá articularse con el mandato contenido en el artículo 10 de la Constitución y con las políticas nacionales de desarrollo territorial.

#### **Artículo 87.- Articulación con la Zona Especial de Desarrollo Integral Fronterizo.**

Las actuaciones realizadas al amparo de esta ley deberán coordinarse con la Ley núm. 12-21, que crea la Zona Especial de Desarrollo Integral Fronterizo, y con los órganos responsables de su implementación.

La presente ley no modificará los requisitos, beneficios, incentivos, procedimientos de clasificación ni períodos de vigencia establecidos por dicho régimen.

Los proyectos productivos vinculados a Frontera Inteligente RD que pretendan beneficiarse del régimen de la Ley núm. 12-21 deberán cumplir separadamente los requisitos establecidos en esa legislación.

#### **Artículo 88.- Desarrollo de capacidades productivas y tecnológicas.**

Las instituciones competentes procurarán que la modernización fronteriza genere oportunidades para la formación y participación de trabajadores, técnicos, pequeñas empresas, productores y proveedores establecidos en las provincias fronterizas.

Los programas de capacitación podrán comprender áreas relacionadas con logística, redes, telecomunicaciones, electricidad, mantenimiento tecnológico, sistemas no tripulados, refrigeración, ciberseguridad, analítica de datos y otras competencias necesarias para la operación de infraestructura moderna.

La participación local deberá basarse en capacidad, formación y cumplimiento de los requisitos aplicables y no podrá utilizarse para excluir injustificadamente la competencia o alterar los procedimientos de contratación pública.

#### **Artículo 89.- Encadenamientos económicos.**

Los centros logísticos, mercados, instalaciones comerciales y demás infraestructuras vinculadas con esta política deberán procurar la generación de encadenamientos con productores y empresas nacionales, particularmente aquellos localizados en la región fronteriza.

Las instituciones responsables podrán promover mecanismos de asistencia técnica, asociatividad, formalización, acceso a información comercial y articulación con cadenas de suministro, dentro de sus respectivas competencias.

La política procurará que el desarrollo económico de las provincias fronterizas no dependa exclusivamente del comercio transfronterizo, promoviendo igualmente su conexión con los mercados nacionales e internacionales.

#### **Artículo 90.- Evaluación del impacto territorial.**

Los programas e inversiones relevantes ejecutados dentro de la zona fronteriza deberán incorporar indicadores que permitan evaluar su contribución al empleo formal, inversión, actividad productiva, conectividad y demás resultados territoriales relacionados con su finalidad.

La existencia de incentivos o inversiones públicas no deberá evaluarse únicamente por el monto ejecutado o el número de proyectos aprobados, sino también por los resultados económicos y sociales efectivamente producidos.

Las evaluaciones deberán coordinarse con las instituciones responsables de planificación, desarrollo fronterizo y estadísticas oficiales.

## **CAPÍTULO XIX**

### **INFRAESTRUCTURA ENERGÉTICA Y TELECOMUNICACIONES**

#### **Artículo 91.- Infraestructura crítica de soporte.**

La disponibilidad de energía eléctrica y telecomunicaciones será considerada condición esencial para la operación continua de SIGFRO-RD.

El Plan Maestro deberá identificar los puntos cuya importancia para la seguridad y control fronterizo requiera niveles reforzados de disponibilidad energética y de comunicaciones.

Las soluciones deberán diseñarse conforme a las regulaciones sectoriales vigentes y bajo criterios de resiliencia, redundancia y sostenibilidad.

#### **Artículo 92.- Suministro energético y respaldo.**

Los componentes críticos deberán contar con mecanismos de respaldo energético proporcionales a su función, ubicación, riesgos y tiempo requerido de continuidad.

Las soluciones podrán combinar suministro de red, almacenamiento, generación de emergencia o fuentes renovables cuando técnica, económica y ambientalmente resulten apropiadas.

La planificación energética deberá coordinarse con el Ministerio de Energía y Minas y las demás autoridades y empresas del sector eléctrico dentro de sus respectivas competencias, conforme a la Ley General de Electricidad núm. 125-01, modificada por la Ley núm. 186-07, y demás normativa vigente.

#### **Artículo 93.- Telecomunicaciones fronterizas.**

Las redes utilizadas por SIGFRO-RD deberán procurar conectividad segura y redundante mediante las tecnologías que resulten técnicamente adecuadas para cada zona.

La instalación y operación de redes y servicios de telecomunicaciones, así como la utilización del espectro radioeléctrico, estarán sujetas a la Ley General de Telecomunicaciones núm. 153-98 y a las disposiciones emitidas por INDOTEL.

La utilización operacional de frecuencias, redes privadas, enlaces satelitales u otras tecnologías no eximirá del cumplimiento de las autorizaciones legalmente exigibles.

#### **Artículo 94.- Redundancia y comunicaciones de contingencia.**

Los puntos de mayor criticidad deberán disponer, cuando resulte técnica y económicamente razonable, de medios alternativos de comunicación capaces de mantener las funciones esenciales ante la interrupción de la red principal.

Los sistemas de contingencia deberán probarse periódicamente y no limitarse a existir formalmente en los inventarios institucionales.

La pérdida de conectividad deberá activar procedimientos que permitan continuar temporalmente las funciones esenciales y sincronizar posteriormente la información producida durante la contingencia.

#### **Artículo 95.- Aprovechamiento compartido de infraestructura.**

Las instituciones públicas deberán procurar, cuando resulte técnica y jurídicamente viable, compartir torres, ductos, fibra, energía, instalaciones y demás infraestructura de soporte, evitando duplicidades innecesarias.

El uso compartido deberá respetar los niveles de seguridad requeridos y no podrá comprometer la independencia operacional de sistemas críticos.

Las inversiones destinadas primordialmente a SIGFRO-RD podrán generar beneficios adicionales de conectividad para las comunidades fronterizas cuando ello sea compatible con la seguridad de las redes y con el régimen regulatorio de telecomunicaciones.

## **CAPÍTULO XX**

### **FINANCIAMIENTO, INVERSIÓN Y SOSTENIBILIDAD ECONÓMICA**

#### **Artículo 96.- Programación financiera plurianual.**

La ejecución de Frontera Inteligente RD deberá sustentarse en una programación financiera plurianual que permita vincular las prioridades establecidas en el Plan Maestro con el Presupuesto General del Estado y con los instrumentos nacionales de planificación e inversión pública.

La programación deberá incluir no solo los costos de construcción o adquisición, sino también los gastos previsibles de operación, mantenimiento, conectividad, licencias, capacitación, ciberseguridad, actualización y reposición.

No deberá autorizarse la incorporación de un componente crítico sin identificar razonablemente la fuente de financiamiento necesaria para sostenerlo durante su vida operacional.

#### **Artículo 97.- Inversión pública.**

Los proyectos sujetos al Sistema Nacional de Planificación e Inversión Pública deberán cumplir las disposiciones de la Ley núm. 498-06 y las competencias actualmente atribuidas al Ministerio de Hacienda y Economía.

Su incorporación al Plan Maestro o su reconocimiento como prioridad de la Comisión no sustituirá la evaluación, registro, priorización y autorización exigidos por el régimen de inversión pública.

La planificación y ejecución financiera deberá igualmente observar las disposiciones de la Ley Orgánica de Presupuesto núm. 423-06, la legislación sobre administración financiera del Estado y las demás normas vigentes.

#### **Artículo 98.- Fuentes de financiamiento.**

Los proyectos podrán financiarse mediante recursos presupuestarios, crédito público legalmente autorizado, cooperación internacional, donaciones, inversión privada y otros mecanismos permitidos por el ordenamiento jurídico.

La utilización de crédito público deberá sujetarse a la Ley núm. 6-06 y a los análisis de sostenibilidad correspondientes.

Las donaciones de equipos o soluciones tecnológicas deberán ser previamente evaluadas desde el punto de vista de interoperabilidad, seguridad, mantenimiento, vida útil y costo futuro para el Estado.

La gratuidad inicial de una tecnología no constituirá por sí sola justificación suficiente para su incorporación a SIGFRO-RD.

#### **Artículo 99.- Alianzas público-privadas.**

Los proyectos de infraestructura o servicios relacionados con esta política que sean susceptibles de estructuración mediante alianzas público-privadas podrán acogerse al régimen general establecido por la Ley núm. 47-20 y su normativa de aplicación, o por la legislación que en el futuro la modifique o sustituya.

La presente ley no crea un régimen especial de alianzas público-privadas para la frontera.

Las funciones que impliquen ejercicio directo de potestades soberanas, coercitivas, migratorias, aduaneras, sancionadoras o de inteligencia permanecerán bajo responsabilidad de las autoridades públicas competentes, aun cuando infraestructura o servicios auxiliares sean suministrados por entidades privadas.

#### **Artículo 100.- Contratación y costo total de propiedad.**

Las adquisiciones de bienes, servicios y obras necesarias para SIGFRO-RD deberán realizarse conforme a la Ley núm. 47-25 de Contrataciones Públicas, su reglamentación y demás disposiciones vigentes.

La evaluación económica de tecnologías deberá considerar el costo total de propiedad y no únicamente el precio inicial de adquisición.

Los pliegos y contratos deberán contemplar, cuando resulte pertinente, niveles de servicio, mantenimiento, actualización, ciberseguridad, disponibilidad de repuestos, portabilidad de datos, transferencia de conocimientos y condiciones de terminación o migración tecnológica.

La seguridad nacional no podrá invocarse de manera genérica para excluir los mecanismos de control, fiscalización y rendición de cuentas establecidos por la legislación.

## CAPÍTULO XXI

### INDICADORES, EVALUACIÓN, AUDITORÍA Y RENDICIÓN DE CUENTAS

#### **Artículo 101.- Sistema de indicadores.**

La Política Nacional contará con un sistema de indicadores destinado a medir resultados operacionales, tecnológicos, económicos, institucionales y de seguridad.

Los indicadores deberán partir de líneas base verificables y permitir comparar razonablemente la situación anterior y posterior a las intervenciones realizadas.

No se considerará suficiente para evaluar el éxito de la política el número de equipos adquiridos, kilómetros cubiertos o recursos ejecutados cuando estos datos no se relacionen con resultados funcionales.

#### **Artículo 102.- Evaluación de resultados.**

La Comisión deberá conocer periódicamente los resultados consolidados de la Política Nacional y evaluar el grado de cumplimiento del Plan Maestro.

La evaluación deberá considerar, entre otros aspectos, la disponibilidad de los sistemas, tiempos de respuesta, eficiencia de los procedimientos, incidentes, integridad institucional, facilitación del comercio y efectos territoriales.

Las metas cuantitativas específicas serán establecidas en el Plan Maestro y en los instrumentos de planificación correspondientes, procurando que sean medibles, verificables y ajustables cuando exista justificación técnica.

#### **Artículo 103.- Evaluación independiente.**

Los componentes clasificados como críticos, de alto impacto o de especial relevancia presupuestaria deberán ser sometidos periódicamente a evaluaciones independientes de desempeño, impacto, seguridad, interoperabilidad o calidad, según corresponda.

La Comisión determinará la periodicidad y alcance de las evaluaciones atendiendo a la criticidad, nivel de inversión, riesgos y consecuencias potenciales del componente evaluado.

La evaluación no deberá ser realizada exclusivamente por el mismo proveedor encargado del diseño, desarrollo u operación del componente cuando ello pueda comprometer la independencia de sus conclusiones.

Los hallazgos relevantes deberán generar planes de mejora, responsables y mecanismos de seguimiento.

#### **Artículo 104.- Control interno y fiscalización externa.**

Los recursos, procesos y activos destinados a la implementación de esta ley estarán sujetos al Sistema Nacional de Control Interno establecido por la Ley núm. 10-07 y al control externo ejercido por la Cámara de Cuentas conforme a la Constitución y la Ley núm. 18-24.

La naturaleza tecnológica, militar o sensible de un proyecto no eliminará las responsabilidades de control financiero y administrativo, sin perjuicio de las medidas especiales necesarias para proteger información legítimamente clasificada.

La fiscalización deberá poder verificar no solo la existencia documental de una adquisición, sino también, cuando corresponda, la instalación, funcionamiento, disponibilidad y utilización efectiva de los activos financiados con recursos públicos.

#### **Artículo 105.- Transparencia y rendición pública.**

La Comisión promoverá la publicación periódica de información agregada sobre avance físico, ejecución financiera, disponibilidad general, indicadores y principales resultados de la Política Nacional.

No serán objeto de publicación aquellas informaciones cuya divulgación pueda revelar capacidades operacionales, vulnerabilidades, ubicaciones sensibles, fuentes de inteligencia, datos personales protegidos o elementos cuya reserva se encuentre legalmente justificada.

La clasificación de información no deberá extenderse a datos presupuestarios, contractuales o de resultados que puedan divulgarse razonablemente sin comprometer la finalidad protegida.

## **CAPÍTULO XXII**

### **IMPLEMENTACIÓN PROGRESIVA DE LA POLÍTICA NACIONAL**

#### **Artículo 106.- Principio de implementación progresiva.**

La implementación nacional de SIGFRO-RD será progresiva y estará basada en diagnóstico, pruebas, evaluación y ampliación gradual.

No deberá desplegarse de manera general una tecnología o procedimiento crítico sin haber comprobado previamente, cuando la naturaleza del componente lo permita, su funcionalidad, interoperabilidad, ciberseguridad, sostenibilidad y capacidad operacional.

La secuencia de implementación será establecida en el Plan Maestro.

#### **Artículo 107.- Etapa preparatoria.**

Durante la etapa inicial deberán completarse el inventario tecnológico, línea base, arquitectura de interoperabilidad, diagnóstico jurídico, evaluación de riesgos, planificación financiera y definición de las responsabilidades institucionales necesarias para comenzar la implementación.

Los sistemas y proyectos que ya se encuentren válidamente operativos al entrar en vigencia esta ley no deberán suspenderse por la realización de este proceso y serán incorporados progresivamente a la nueva arquitectura cuando resulte compatible.

#### **Artículo 108.- Proyectos piloto.**

Las tecnologías o procesos cuya escala, complejidad o impacto aconsejen validación previa podrán implementarse inicialmente mediante proyectos piloto en uno o más puntos fronterizos seleccionados conforme a criterios técnicos.

Los pilotos deberán permitir evaluar el funcionamiento completo del procedimiento y no únicamente el rendimiento aislado del equipo adquirido.

Antes de su expansión deberán documentarse los resultados, costos, fallas, incidentes, necesidades de capacitación y modificaciones requeridas.

#### **Artículo 109.- Expansión condicionada a resultados.**

La ampliación de un componente hacia nuevos puntos o zonas fronterizas deberá tomar en consideración los resultados obtenidos durante las etapas anteriores.

El Plan Maestro establecerá mecanismos de aprobación por etapas que permitan continuar, corregir, rediseñar o suspender una expansión cuando existan problemas significativos de seguridad, funcionamiento, interoperabilidad, sostenibilidad financiera o respeto de derechos.

El cumplimiento de una fecha prevista no obligará por sí mismo a expandir un componente que no haya alcanzado condiciones razonables de funcionamiento.

#### **Artículo 110.- Consolidación y operación permanente.**

Completada la etapa inicial de despliegue, SIGFRO-RD entrará en un ciclo permanente de operación, mantenimiento, evaluación, actualización y reposición tecnológica.

La culminación de los proyectos iniciales no extinguirá las responsabilidades establecidas por esta ley ni convertirá la política en un programa temporal.

El Poder Ejecutivo deberá procurar que los instrumentos nacionales de planificación mantengan la seguridad, tecnificación y desarrollo de la zona fronteriza dentro de las prioridades permanentes del Estado, de conformidad con el mandato constitucional.

## CAPÍTULO XXIII

### RESPONSABILIDAD, USO INDEBIDO Y PROTECCIÓN DE LA INTEGRIDAD DE SIGFRO-RD

#### **Artículo 111.- Deber de utilización legítima.**

Los funcionarios, servidores públicos, contratistas, proveedores y demás personas que tengan acceso autorizado a SIGFRO-RD estarán obligados a utilizar sus sistemas, datos, equipos y servicios exclusivamente para las finalidades vinculadas con las funciones o actividades que justificaron dicho acceso.

El acceso autorizado a un sistema no conferirá facultad para consultar información ajena a la función desempeñada ni para utilizarla con fines personales, políticos, comerciales o distintos de los legalmente permitidos.

Toda persona con acceso al sistema estará sometida a los deberes de confidencialidad, seguridad, integridad y trazabilidad que correspondan conforme a la naturaleza de la información tratada.

#### **Artículo 112.- Conductas prohibidas.**

Queda prohibida la alteración, ocultamiento, eliminación, extracción, divulgación, copia, utilización o transmisión no autorizada de información obtenida mediante SIGFRO-RD.

Se prohíbe igualmente facilitar credenciales a terceros, evadir controles tecnológicos, desactivar injustificadamente mecanismos de seguridad, incorporar información deliberadamente falsa, modificar ilícitamente alertas, manipular resultados, destruir registros de auditoría o utilizar sistemas o privilegios administrativos para impedir la trazabilidad de una actuación.

La presente disposición se aplicará sin perjuicio de las responsabilidades previstas en la legislación penal, administrativa, disciplinaria, civil, militar o contractual correspondiente.

#### **Artículo 113.- Preservación de registros ante posibles irregularidades.**

Cuando se detecten indicios razonables de manipulación, acceso no autorizado, alteración de registros, filtración de información, sabotaje, fraude u otra conducta que pueda generar responsabilidad, la institución competente deberá adoptar las medidas necesarias para preservar los registros y demás elementos técnicos relacionados con el hecho.

La preservación deberá realizarse procurando mantener la integridad, autenticidad y trazabilidad de la información y evitando alteraciones que puedan afectar una investigación posterior.

Cuando los hechos puedan constituir una infracción penal, deberán ponerse en conocimiento del Ministerio Público o del organismo de investigación competente conforme al ordenamiento jurídico.

**Artículo 114.- Régimen de responsabilidad.**

El incumplimiento de las obligaciones establecidas en esta ley podrá generar responsabilidad administrativa, disciplinaria, civil, penal, militar o contractual, según corresponda a la naturaleza de la conducta y a la condición de la persona responsable.

Las sanciones únicamente podrán ser impuestas por las autoridades competentes, conforme a la Constitución, las leyes y el debido procedimiento.

La presente ley no crea tipos penales mediante interpretación extensiva. Las conductas constitutivas de infracciones penales serán perseguidas conforme a la Ley Orgánica núm. 74-25, que instituye el Código Penal de la República Dominicana, modificada por la Ley núm. 44-26, la Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología y las demás disposiciones penales especiales que resulten aplicables.

**Párrafo.-** La determinación de responsabilidades respetará las garantías del debido proceso y los principios aplicables a la prohibición de doble persecución o sanción por una misma causa.

**Artículo 115.- Reporte de incidentes e irregularidades.**

Los servidores públicos que, en ejercicio de sus funciones, tengan conocimiento de incidentes graves de seguridad, alteraciones deliberadas, accesos ilegítimos o posibles actos de corrupción relacionados con SIGFRO-RD deberán comunicarlos por los canales institucionales establecidos.

Las instituciones deberán habilitar mecanismos seguros para recibir, documentar y tramitar estos reportes y preservar, dentro de los límites establecidos por la ley, la confidencialidad de la información y de las personas que legítimamente comuniquen hechos sujetos a investigación.

La recepción de una denuncia o alerta no constituirá prueba de responsabilidad ni permitirá imponer sanciones sin el procedimiento correspondiente.

## CAPÍTULO XXIV

### PROTECCIÓN, CONSERVACIÓN Y ACCESO A LOS DATOS

#### **Artículo 116.- Principios aplicables al tratamiento de datos.**

El tratamiento de datos personales mediante SIGFRO-RD deberá responder a una finalidad legítima, determinada y vinculada con las competencias de la institución que los utilice.

La recopilación, consulta, intercambio y conservación deberán limitarse a la información necesaria y proporcional para cumplir dicha finalidad, observando el artículo 44 de la Constitución, la Ley núm. 172-13 sobre Protección Integral de los Datos Personales y los regímenes especiales aplicables.

La integración tecnológica entre instituciones no convertirá la totalidad de sus bases de datos en una fuente de consulta general para todos los organismos participantes.

#### **Artículo 117.- Datos de protección reforzada.**

Los datos biométricos y demás categorías de información cuya naturaleza pueda generar riesgos significativos para la intimidad, identidad o seguridad de una persona estarán sometidos a medidas reforzadas de protección.

Su almacenamiento y tratamiento deberán incorporar controles estrictos de acceso, cifrado u otras medidas de seguridad apropiadas, registro de consultas y procedimientos de respuesta frente a accesos no autorizados.

Las plantillas biométricas originales no deberán ser distribuidas entre instituciones cuando la finalidad pueda cumplirse mediante un mecanismo seguro de verificación o respuesta limitada.

#### **Artículo 118.- Conservación diferenciada.**

SIGFRO-RD no utilizará un único período de conservación para todas las categorías de información.

Los plazos deberán establecerse atendiendo a la finalidad del tratamiento, naturaleza del dato, legislación sectorial aplicable, obligaciones de archivo, existencia de investigaciones o procedimientos y necesidades legítimas de seguridad y auditoría.

Cuando haya desaparecido la finalidad legítima de conservación y no exista obligación jurídica que exija mantener la información, esta deberá eliminarse, anonimizarse o someterse al tratamiento que corresponda conforme al ordenamiento jurídico.

**Párrafo.-** La existencia de una investigación administrativa, penal, judicial, de auditoría o de ciberseguridad podrá justificar la preservación temporal de información relacionada con ella hasta que legalmente deje de ser necesaria.

**Artículo 119.- Derechos sobre la información personal.**

Las personas podrán ejercer los derechos que les reconozcan la Constitución y la legislación vigente respecto de los datos personales tratados por las instituciones participantes.

Cuando la información provenga de una institución fuente, las solicitudes de acceso, rectificación, actualización o demás actuaciones relativas al dato deberán ser tramitadas ante dicha institución o mediante el procedimiento legalmente establecido.

El ejercicio de estos derechos estará sujeto a las excepciones y limitaciones previstas por la Constitución y las leyes en materias tales como seguridad nacional, defensa, inteligencia, prevención e investigación de infracciones y procesos judiciales.

**Párrafo.-** SIGFRO-RD deberá disponer de mecanismos que permitan reflejar las rectificaciones realizadas válidamente por las instituciones fuente sin eliminar indebidamente la trazabilidad histórica cuando esta deba conservarse.

**Artículo 120.- Comunicación internacional de información.**

La información obtenida mediante SIGFRO-RD no podrá ser entregada a gobiernos extranjeros, organismos internacionales o entidades privadas extranjeras por el solo hecho de participar en actividades de cooperación fronteriza.

Toda comunicación internacional de datos deberá tener fundamento en la Constitución, una ley, tratado, acuerdo internacional, mecanismo de cooperación jurídicamente válido o atribución legal de la autoridad que realiza la transferencia.

La información compartida deberá limitarse a la necesaria para la finalidad autorizada y estará sujeta a las medidas de seguridad y restricciones de utilización correspondientes.

**Párrafo I.-** Ninguna autoridad extranjera tendrá acceso directo y general a SIGFRO-RD ni a las bases de datos de las instituciones dominicanas por virtud de esta ley.

**Párrafo II.-** Las disposiciones de este artículo se entenderán sin perjuicio de los mecanismos legalmente vigentes de cooperación migratoria, aduanera, policial, judicial, sanitaria, ambiental, de inteligencia o de seguridad.

**Artículo 121.- Datos estadísticos y transparencia.**

Las instituciones podrán producir estadísticas, estudios e indicadores derivados de SIGFRO-RD procurando utilizar información agregada o anonimizada cuando la identificación individual no resulte necesaria.

La publicación de información se realizará conforme a la Ley núm. 200-04 sobre Libre Acceso a la Información Pública y demás normas aplicables, preservando los datos personales, información clasificada, secretos legalmente protegidos, vulnerabilidades tecnológicas y elementos cuya divulgación pueda comprometer operaciones legítimas de seguridad.

La invocación de razones de seguridad deberá aplicarse de manera específica y proporcional y no constituirá fundamento para ocultar información administrativa o financiera que legalmente deba ser pública.

## **CAPÍTULO XXV**

### **DESARROLLO REGLAMENTARIO Y NORMATIVO**

#### **Artículo 122.- Reglamento General.**

El Poder Ejecutivo dictará el Reglamento General de Aplicación de la presente ley dentro de los ciento ochenta días siguientes a su entrada en vigencia.

El Reglamento desarrollará los mecanismos necesarios para la coordinación, interoperabilidad, gestión de eventos, seguridad, protección de información, evaluación y demás materias cuya regulación resulte necesaria para la ejecución de esta ley, sin alterar las competencias atribuidas legalmente a las instituciones participantes.

El ejercicio de la potestad reglamentaria no podrá crear delitos, sanciones, tributos, categorías migratorias ni restricciones de derechos que requieran disposición legal.

#### **Artículo 123.- Normas técnicas.**

Las autoridades rectoras competentes podrán emitir o actualizar las normas técnicas necesarias para la aplicación de esta ley dentro de los ámbitos que legalmente les correspondan.

Las materias de interoperabilidad y transformación digital deberán armonizarse con las NORTIC vigentes; la ciberseguridad se regirá por el marco nacional aplicable y las disposiciones de las autoridades competentes; y las materias aeronáuticas, de telecomunicaciones, ambientales, sanitarias y demás sectores especializados continuarán sometidas a sus respectivos regímenes regulatorios.

Las normas técnicas no podrán modificar las competencias ni garantías establecidas por esta ley.

#### **Artículo 124.- Protocolos interinstitucionales.**

Las instituciones participantes adoptarán los protocolos necesarios para regular las operaciones en las que intervengan dos o más organismos.

Estos protocolos podrán establecer flujos de información, responsables operacionales, procedimientos de coordinación, niveles de acceso, contingencias y mecanismos de escalamiento, siempre dentro de las competencias establecidas por el ordenamiento jurídico.

Los protocolos deberán mantenerse actualizados y estarán sujetos a revisión cuando cambien los sistemas, riesgos, procedimientos o disposiciones legales que les sirven de fundamento.

#### **Artículo 125.- Evaluación jurídica previa de nuevos usos tecnológicos.**

Antes de incorporar de manera permanente una tecnología que implique nuevas formas de tratamiento biométrico, vigilancia automatizada, inteligencia artificial de alto impacto o intercambio masivo de información, la institución responsable deberá realizar una evaluación jurídica y de riesgos adecuada a la naturaleza del proyecto.

La evaluación deberá determinar la competencia legal, finalidad, proporcionalidad, categorías de información involucradas, posibles impactos sobre derechos fundamentales, medidas de seguridad y necesidad de regulación adicional.

Cuando la tecnología exceda las facultades reconocidas por el ordenamiento vigente, su implementación deberá esperar la adopción del instrumento jurídico correspondiente.

#### **Artículo 126.- Neutralidad y actualización tecnológica.**

Los reglamentos, normas técnicas y protocolos derivados de esta ley deberán procurar formular requisitos funcionales, de seguridad, interoperabilidad y desempeño sin incorporar innecesariamente marcas, fabricantes, modelos o tecnologías propietarias.

La sustitución de una tecnología por otra que cumpla las mismas funciones no requerirá modificación de esta ley cuando permanezcan inalterados los derechos, competencias, controles y finalidades establecidos en ella.

La regulación técnica deberá revisarse periódicamente para evitar que la obsolescencia tecnológica comprometa la seguridad o funcionamiento de SIGFRO-RD.

## CAPÍTULO XXVI

### DISPOSICIONES TRANSITORIAS DE IMPLEMENTACIÓN

#### **Artículo 127.- Constitución inicial de la Comisión.**

La Comisión Interinstitucional para la Frontera Inteligente deberá quedar formalmente constituida dentro de los noventa días siguientes a la entrada en vigencia de la presente ley.

Durante su primera etapa identificará los enlaces institucionales, establecerá su mecanismo interno de funcionamiento y organizará la Secretaría Técnica Interinstitucional utilizando las estructuras existentes.

La constitución de la Comisión no será condición para que las instituciones continúen ejecutando las funciones que les hayan sido atribuidas por la legislación vigente.

#### **Artículo 128.- Continuidad de los sistemas existentes.**

Los sistemas, infraestructuras, programas y proyectos fronterizos existentes al momento de entrar en vigencia esta ley continuarán operando conforme a sus respectivos marcos jurídicos.

Su incorporación a SIGFRO-RD será progresiva y estará condicionada a la evaluación de compatibilidad, interoperabilidad, ciberseguridad y necesidad operacional correspondiente.

La entrada en vigencia de esta ley no suspenderá los servicios migratorios, aduaneros, militares, sanitarios, de vigilancia o de cualquier otra naturaleza que actualmente presten las instituciones competentes.

#### **Artículo 129.- Inventario inicial.**

Las instituciones participantes deberán remitir la información necesaria para elaborar el inventario tecnológico inicial dentro de los ciento ochenta días siguientes a la constitución de la Comisión, sin perjuicio de la información cuya naturaleza requiera canales especiales de seguridad.

La Secretaría Técnica consolidará la información y establecerá los mecanismos para su actualización permanente.

Las diferencias entre el inventario técnico creado por esta ley y los registros patrimoniales institucionales deberán ser conciliadas sin sustituir las obligaciones contables y administrativas aplicables.

#### **Artículo 130.- Primer Plan Maestro.**

El primer Plan Maestro de Frontera Inteligente deberá ser elaborado dentro de los doce meses siguientes a la constitución de la Comisión.

El Plan establecerá el diagnóstico inicial, arquitectura objetivo, prioridades de integración y cronograma progresivo de implementación, tomando en consideración los sistemas y proyectos que se encuentren operativos o en ejecución.

Los proyectos cuya continuidad sea necesaria para la seguridad o funcionamiento de la frontera no deberán paralizarse a la espera de la aprobación del Plan, pero deberán procurar su futura compatibilidad con la arquitectura establecida por esta ley.

**Artículo 131.- Contratos y situaciones jurídicas existentes.**

Los contratos, autorizaciones, licencias, concesiones, convenios y demás situaciones jurídicas válidamente constituidas antes de la entrada en vigencia de esta ley conservarán sus efectos conforme al ordenamiento aplicable.

Las instituciones deberán procurar que las renovaciones, ampliaciones o nuevas contrataciones relacionadas con SIGFRO-RD se adapten progresivamente a los requisitos de interoperabilidad, seguridad, portabilidad, mantenimiento y trazabilidad establecidos por esta ley.

Ninguna adaptación podrá modificar retroactivamente derechos y obligaciones válidamente constituidos fuera de los mecanismos autorizados por el ordenamiento jurídico.

## **CAPÍTULO XXVII**

### **DISPOSICIONES FINALES**

**Artículo 132.- Naturaleza orgánica.**

La presente ley es de naturaleza orgánica por regular materias vinculadas con la seguridad y defensa nacional y establecer disposiciones relacionadas con el ejercicio y protección de derechos fundamentales, de conformidad con el artículo 112 de la Constitución de la República Dominicana.

Su aprobación o modificación requerirá el voto favorable de las dos terceras partes de los presentes en cada cámara legislativa.

**Artículo 133.- Aplicación complementaria de la legislación sectorial.**

La presente ley deberá interpretarse y aplicarse conjuntamente con la Constitución de la República y con las disposiciones legales que regulan migración, aduanas, Fuerzas Armadas, inteligencia, administración pública, función pública, procedimiento administrativo, protección de datos personales, documentos y firmas digitales, cibercriminalidad, salud, sanidad agropecuaria, medio ambiente, telecomunicaciones, aviación civil, contratación pública, planificación, presupuesto, inversión pública y demás materias relacionadas.

En materia de inteligencia y seguridad de los sistemas estatales se aplicará, dentro de su ámbito, la Ley núm. 1-26, Orgánica que crea la Dirección Nacional de Inteligencia y regula el Sistema Nacional de Inteligencia, así como sus disposiciones reglamentarias.

Cuando una legislación especial atribuya una competencia determinada a una autoridad específica, dicha atribución prevalecerá dentro de su ámbito material.

**Artículo 134.- Preservación de competencias y regímenes existentes.**

La presente ley no deroga ni sustituye, salvo disposición expresa en contrario, las competencias establecidas por la Ley General de Migración núm. 285-04, la Ley General de Aduanas núm. 168-21, la Ley Orgánica de las Fuerzas Armadas núm. 139-13, la legislación que regula el Sistema Nacional de Inteligencia, la Ley núm. 12-21 de Desarrollo Fronterizo ni los demás regímenes sectoriales relacionados con la gestión fronteriza.

Las disposiciones deberán interpretarse de manera que se preserve la especialidad de dichos regímenes y se facilite su coordinación mediante SIGFRO-RD.

Cuando se identifique una incompatibilidad normativa que no pueda solucionarse mediante interpretación armónica, deberá utilizarse el procedimiento constitucional y legislativo correspondiente para su modificación, evitando derogaciones implícitas de competencias esenciales.

**Artículo 135.- Evaluación integral de la ley.**

Transcurridos cinco años desde la entrada en vigencia de la presente ley, el Poder Ejecutivo deberá disponer una evaluación integral de su implementación.

La evaluación examinará los resultados en materia de seguridad, interoperabilidad, gestión migratoria y aduanera, ciberseguridad, protección de derechos, integridad institucional, eficiencia del gasto y desarrollo fronterizo.

Sus resultados deberán servir para determinar la necesidad de mantener, modificar, ampliar o derogar disposiciones cuya experiencia práctica haya demostrado insuficiencias, duplicidades o efectos no previstos.

La evaluación no impedirá que antes de dicho plazo se propongan modificaciones legislativas cuando exista una necesidad debidamente justificada.

**Artículo 136.- Entrada en vigencia.**

La presente ley entrará en vigencia conforme a las disposiciones del artículo 109 de la Constitución de la República Dominicana, una vez promulgada, publicada y transcurridos los plazos legalmente establecidos para que se repute conocida en todo el territorio nacional.