DOCUMENTO MARCO

POLÍTICA NACIONAL PARA LA TECNIFICACIÓN Y GESTIÓN INTEGRAL DE LA FRONTERA DOMINICO-HAITIANA

ANT-LEG-05 "FRONTERA INTELIGENTE RD"

RD PROPONE
Ideas de hoy para un mejor mañana

CAPÍTULO I

INTRODUCCIÓN, ANTECEDENTES Y JUSTIFICACIÓN

1.1. Introducción

La frontera terrestre entre la República Dominicana y la República de Haití constituye uno de los espacios de mayor importancia estratégica para la soberanía, la seguridad nacional, el comercio, la migración, la salud pública, la protección ambiental y el desarrollo territorial dominicano.

Su gestión no puede ser concebida exclusivamente desde una perspectiva militar ni reducirse a la construcción de infraestructuras físicas destinadas a impedir cruces irregulares. La complejidad de las relaciones fronterizas exige un sistema capaz de gestionar simultáneamente personas, vehículos, mercancías, riesgos sanitarios, actividades económicas, amenazas ambientales y situaciones relacionadas con la seguridad nacional.

La Constitución de la República Dominicana proclamada el 27 de octubre de 2024 ofrece un fundamento particularmente sólido para una política de esta naturaleza. Su artículo 10 declara de **supremo y permanente interés nacional** la seguridad y el desarrollo económico, social y turístico de la Zona Fronteriza, así como su integración vial, comunicacional y productiva, ordenando a los poderes públicos elaborar, ejecutar y priorizar políticas e inversiones destinadas a esos objetivos.

Consecuentemente, la tecnificación fronteriza no debe ser entendida únicamente como una política de seguridad. Constituye simultáneamente una política de soberanía, modernización del Estado, desarrollo regional, formalización económica y transformación digital.

1.2. Antecedentes

Durante las últimas décadas, la República Dominicana ha fortalecido progresivamente su presencia institucional en la zona fronteriza.

La creación del Cuerpo Especializado de Seguridad Fronteriza Terrestre —CESFRONT— mediante el Decreto núm. 325-06 y la posterior asignación de sus áreas de responsabilidad mediante el Decreto núm. 323-07 constituyeron pasos importantes hacia la especialización del control fronterizo. CESFRONT tiene entre sus responsabilidades mantener dispositivos de seguridad y control en los puntos de entrada y salida y desarrollar patrullaje y puestos complementarios en la franja fronteriza.

Posteriormente, el Estado dominicano inició la construcción de una verja perimetral fronteriza concebida progresivamente como infraestructura inteligente. La primera fase contempló aproximadamente 54 kilómetros de verja física, vías para patrullaje, torres de vigilancia y accesos operativos. En 2025 comenzó una ampliación de 13 kilómetros en Dajabón y, el 5 de septiembre de 2026, se inició la construcción de otros 14.5 kilómetros en Jimaní.

Paralelamente, se han incorporado soluciones tecnológicas como fibra óptica, cámaras térmicas, cámaras de visión diurna y nocturna, sensores de movimiento, radares, torres de comunicaciones, drones y centros de comando vinculados al C5i de las Fuerzas Armadas.

También se observan avances sectoriales.

La Dirección General de Migración ha desarrollado procesos de captura y verificación biométrica, incluyendo reconocimiento facial y huellas dactilares en los principales puntos fronterizos, mientras su programación institucional para 2026 contempla infraestructura destinada a biometrizar y capturar datos de quienes participan en mercados binacionales.

Por su parte, la Dirección General de Aduanas desarrolla el Proyecto de Identificación Vehicular Fronteriza —IVF-RD—, mediante tecnologías RFID, códigos QR, holografía y una plataforma centralizada de registro, seguridad e inteligencia aduanal interoperable con otros organismos estatales.

Estos avances evidencian que el país ha comenzado un proceso real de transformación tecnológica de su frontera.

Sin embargo, también revelan una oportunidad fundamental que es integrar esas capacidades dentro de un modelo nacional único de gestión fronteriza.

1.3. Problema central

El desafío dominicano ya no consiste únicamente en adquirir cámaras, drones, sistemas biométricos o equipos de inspección.

El desafío consiste en lograr que la cámara detecte, el sistema identifique, las instituciones consulten, la inteligencia evalúe, la autoridad actúe y todo quede registrado.

Cuando cada institución desarrolla sistemas independientes, existe el riesgo de producir múltiples plataformas tecnológicamente avanzadas pero operacionalmente desconectadas.

Esta política propone superar ese modelo. La tecnificación deberá conducir a una frontera donde los procesos físicos y digitales formen parte de una misma cadena de control.

1.4. Justificación

La Política Nacional para la Tecnificación y Gestión Integral de la Frontera Dominico-Haitiana se justifica por cinco razones fundamentales:

a) **Soberanía.** El Estado debe disponer de capacidad permanente para conocer y controlar los movimientos relevantes dentro de su territorio fronterizo;

b) **Seguridad.** Las amenazas relacionadas con tráfico ilícito de personas, contrabando, narcotráfico, armas, mercancías, falsificación documental y crimen organizado requieren capacidades tecnológicas superiores a los controles exclusivamente manuales;

c) **Modernización.** El Estado dominicano posee actualmente infraestructura digital, biométrica, aduanera y de interoperabilidad que permite avanzar hacia un modelo integrado;

d) **Transparencia.** La digitalización permite registrar quién realizó cada operación, cuándo la realizó, qué verificaciones efectuó y bajo qué fundamento autorizó o rechazó una actuación;

e) **Desarrollo.** Una frontera organizada puede facilitar el comercio legítimo, atraer inversión, crear empleos y fortalecer las comunidades fronterizas.

Este último aspecto está expresamente alineado con la Ley núm. 1-12 sobre Estrategia Nacional de Desarrollo 2030, que contempla el fortalecimiento de la presencia institucional del Estado, la capacidad productiva de las comunidades fronterizas, el comercio, la infraestructura logística y la protección ambiental de la zona.

1.5. Objetivo general

Diseñar e implementar un modelo nacional integrado de gestión fronteriza que utilice tecnologías modernas para fortalecer la soberanía, seguridad, control migratorio, fiscalización aduanera, trazabilidad comercial, protección sanitaria y ambiental y desarrollo económico de la frontera dominico-haitiana.

1.6. Objetivos específicos

La política procurará:

a) **Integrar** las capacidades tecnológicas existentes;

b) **Digitalizar** progresivamente los procesos fronterizos;

c) **Identificar** con mayor precisión personas, vehículos y mercancías;

d) **Detectar** automáticamente eventos de riesgo;

e) **Facilitar** el comercio legítimo;

f) **Reducir** oportunidades de corrupción;

g) **Fortalecer** la capacidad operacional de las autoridades;

h) **Garantizar** trazabilidad de las actuaciones;

i) **Proteger** adecuadamente los datos personales;

j) **Mejorar** la coordinación interinstitucional;

k) **Desarrollar** económicamente las comunidades fronterizas;

l) **Evaluar** periódicamente los resultados mediante indicadores verificables.

1.7. Principios rectores

La Política se regirá por los principios de:

a) Legalidad;

b) Soberanía;

c) Proporcionalidad;

d) Interoperabilidad;

e) Seguridad por diseño;

f) Privacidad por diseño;

g) Trazabilidad;

h) Transparencia;

i) Responsabilidad institucional;

j) Continuidad operativa;

k) Neutralidad tecnológica;

l) Desarrollo territorial;

m) Respeto de los derechos fundamentales;

n) Evaluación permanente.

CAPÍTULO II

DIAGNÓSTICO ACTUAL DE LA FRONTERA DOMINICO-HAITIANA

2.1. Caracterización general

La frontera terrestre dominico-haitiana posee aproximadamente 391 kilómetros de extensión, atravesando zonas geográficas con características montañosas, agrícolas, urbanas, rurales, lacustres y costeras.

La actividad estatal se concentra especialmente alrededor de Dajabón, Elías Piña, Jimaní y Pedernales, donde concurren funciones militares, migratorias, aduaneras y comerciales. Esta extensión y diversidad territorial imposibilitan depender exclusivamente de presencia humana permanente.

La tecnología debe convertirse, por tanto, en un multiplicador de la capacidad operacional del Estado.

2.2. Riesgos que debe administrar el sistema

La frontera constituye un espacio en el que pueden coincidir distintas categorías de riesgos:

a) Migración irregular;

b) Tráfico ilícito de migrantes;

c) Trata de personas;

d) Contrabando de mercancías;

e) Tráfico de armas;

f) Narcotráfico;

g) Falsificación documental;

h) Evasión aduanera;

i) Robo o utilización irregular de vehículos;

j) Comercio informal no trazable;

k) Riesgos epidemiológicos;

l) Riesgos fitosanitarios y zoosanitarios;

m) Tala y extracción ilegal de recursos naturales;

n) Delitos ambientales;

o) Corrupción administrativa;

p) Ciberataques contra infraestructura crítica.

CESFRONT reconoce expresamente dentro del contexto de su misión amenazas vinculadas con narcotráfico, tráfico de armas y mercancías, migración irregular, trata de personas y afectaciones ambientales. Por consiguiente, el concepto de seguridad fronteriza debe ampliarse desde la vigilancia física hacia la **gestión integral del riesgo**.

2.3. Fragmentación institucional

En la frontera interactúan diferentes organismos con competencias legítimamente diferenciadas. Entre ellos se encuentran:

a) Ministerio de Defensa;

b) Ejército de República Dominicana;

c) CESFRONT;

d) Dirección General de Migración;

e) Dirección General de Aduanas;

f) Dirección Nacional de Inteligencia, dentro de sus competencias legales;

g) Policía Nacional cuando corresponda;

h) Ministerio de Salud Pública;

i) Ministerio de Agricultura y organismos sanitarios competentes;

j) Ministerio de Medio Ambiente y Recursos Naturales;

k) Ministerio de Relaciones Exteriores;

l) Organismos de investigación y persecución penal cuando corresponda;

m) Gobiernos locales y entidades de desarrollo fronterizo en sus respectivos ámbitos.

El problema no es la existencia de múltiples instituciones. La especialización institucional resulta necesaria. El riesgo aparece cuando sus sistemas, protocolos y bases de información funcionan sin mecanismos suficientes de interoperabilidad.

2.4. El problema de los sistemas aislados

Un vehículo puede ser simultáneamente objeto de interés para Aduanas, Migración, CESFRONT y organismos de seguridad.

Una persona puede interactuar con sistemas migratorios, registros biométricos, controles aduaneros y cámaras de seguridad.

Una carga puede generar información comercial, aduanera, sanitaria y de inteligencia.

Si cada evento produce expedientes independientes, el Estado pierde capacidad para reconocer relaciones entre esos acontecimientos.

Por ello, la frontera inteligente no debe crear una enorme base de datos que sustituya las bases existentes.

Debe crear **capacidad segura de consulta e interoperabilidad entre ellas**.

Esta distinción será fundamental para todo el proyecto.

2.5. Dependencia de procedimientos humanos

Los controles humanos continuarán siendo indispensables, sin embargo, determinadas actuaciones presentan vulnerabilidades cuando dependen exclusivamente de inspecciones manuales. Entre ellas:

a) Comparación visual de documentos;

b) Registro manual de matrículas;

c) Inspección repetitiva de vehículos;

d) Registro manual de movimientos;

e) Confirmación telefónica entre instituciones;

f) Autorizaciones sin trazabilidad electrónica;

g) Verificaciones realizadas sobre documentos impresos;

h) Selección discrecional de personas o mercancías para inspección.

La tecnificación debe reducir esas vulnerabilidades mediante automatización y controles cruzados.

2.6. Cobertura territorial

La construcción de la verja perimetral constituye una herramienta importante, pero no cubre la totalidad de los aproximadamente 391 kilómetros de frontera. Por ello, una política nacional no puede fundamentarse exclusivamente en infraestructura física continua. El modelo deberá combinar:

Barrera física + vigilancia electrónica + movilidad operativa + inteligencia + respuesta rápida.

En zonas sin infraestructura física, sensores terrestres, cámaras de largo alcance, radares, drones y patrullaje basado en riesgo pueden proporcionar cobertura complementaria.

2.7. Desafío económico fronterizo

Otro componente esencial del diagnóstico es la informalidad económica.

El comercio fronterizo constituye una fuente importante de actividad para determinadas comunidades, pero cuanto mayor sea la informalidad, menor será la capacidad estatal de:

a) Conocer las mercancías movilizadas;

b) Determinar correctamente obligaciones aduaneras;

c) Verificar estándares sanitarios;

d) Identificar operadores comerciales;

e) Prevenir contrabando;

f) Producir estadísticas confiables;

g) Facilitar posteriormente el comercio legítimo.

En febrero de 2026 el Poder Ejecutivo anunció la intención de desarrollar una red de puertos secos y centros logísticos fronterizos para organizar y fortalecer el comercio formal. La presente política incorpora esa visión dentro de un sistema tecnológico superior.

2.8. Diagnóstico institucional

La República Dominicana presenta una situación favorable para avanzar hacia la frontera inteligente porque ya dispone de:

a) Infraestructura física fronteriza en expansión;

b) Centros de mando;

c) Fibra óptica;

d) Cámaras térmicas;

e) Sensores;

f) Drones;

g) Sistemas biométricos;

h) Plataformas aduaneras;

i) Sistemas de identificación vehicular en implementación;

j) Capacidad estatal de interoperabilidad;

k) Instituciones especializadas.

El principal déficit identificado no es, por tanto, la inexistencia absoluta de tecnología. Es la ausencia de una arquitectura nacional que conecte progresivamente todas estas capacidades mediante reglas comunes.

2.9. Conclusión diagnóstica

El país se encuentra en una transición de frontera vigilada a una frontera tecnificada. La política propuesta pretende completar una segunda transición **de frontera tecnificada hacia una frontera integrada e inteligente.**

CAPÍTULO III

MARCO CONSTITUCIONAL, LEGAL Y REGLAMENTARIO

3.1. Principio de supremacía constitucional

Toda actuación derivada de esta política deberá encontrarse subordinada a la Constitución de la República Dominicana. La tecnificación fronteriza no otorgará competencias extraordinarias a las autoridades fuera de las previstas constitucional y legalmente.

La tecnología será una herramienta para ejercer competencias existentes con mayor eficacia, trazabilidad y coordinación.

3.2. Constitución de la República

La Constitución de 2024 proporciona varios fundamentos esenciales.

Artículo 10: Régimen fronterizo

Este artículo reviste especial importancia porque declara de supremo y permanente interés nacional la seguridad y el desarrollo económico, social y turístico de la Zona Fronteriza, junto con su integración vial, comunicacional y productiva.

Esta disposición permite fundamentar simultáneamente:

a) Infraestructura tecnológica;

b) Sistemas de comunicaciones;

c) Seguridad territorial;

d) Desarrollo económico;

e) Logística;

f) Integración productiva;

g) Inversión pública prioritaria.

Artículo 11: Tratados fronterizos

Las actuaciones deberán respetar las disposiciones constitucionales y los tratados que regulan aspectos de la delimitación y relaciones fronterizas entre República Dominicana y Haití.

Artículo 44: Intimidad y protección de información personal

La utilización de biometría, reconocimiento facial, registros vehiculares y bases interoperables debe cumplir estrictamente las garantías constitucionales.

El artículo 44 reconoce el derecho de las personas a conocer los datos que sobre ellas reposen en registros públicos o privados y exige que el tratamiento de información personal respete, entre otros, los principios de calidad, licitud, lealtad, seguridad y finalidad. Este artículo será uno de los pilares de la arquitectura tecnológica que posteriormente desarrollará este Documento Marco.

Artículo 252: Fuerzas Armadas

La Constitución atribuye a las Fuerzas Armadas la defensa de la independencia, soberanía e integridad de los espacios geográficos de la Nación.

Por tanto, el componente tecnológico de vigilancia territorial debe reconocer la responsabilidad constitucional militar sin sustituir las atribuciones civiles correspondientes a Migración, Aduanas u otros organismos.

3.3. Ley General de Migración núm. 285-04

La Ley núm. 285-04 constituye la principal base jurídica del control migratorio dominicano.

La Dirección General de Migración es responsable de la aplicación del régimen relativo a entrada, salida, permanencia y categorías migratorias, conjuntamente con su Reglamento de Aplicación aprobado mediante Decreto núm. 631-11.

Consecuentemente, cualquier módulo de control migratorio desarrollado en esta política deberá encontrarse bajo la autoridad legal de Migración.

CESFRONT o cualquier otro organismo podrá colaborar dentro de sus competencias, pero la tecnología no deberá confundir las responsabilidades jurídicas de cada autoridad.

3.4. Ley núm. 137-03 sobre Tráfico Ilícito de Migrantes y Trata de Personas

Esta legislación proporciona fundamentos para prevención, investigación y persecución de actividades relacionadas con tráfico ilícito y trata.

La inteligencia fronteriza deberá contribuir a detectar patrones vinculados con estas conductas, sin sustituir las atribuciones investigativas y judiciales correspondientes.

3.5. Ley General de Aduanas núm. 168-21

La Ley núm. 168-21 modernizó sustancialmente el marco aduanero dominicano. La propia legislación establece mecanismos electrónicos para declaraciones aduaneras y constituye un fundamento importante para automatización, gestión de riesgos y trazabilidad comercial.

Su Reglamento de Aplicación, núm. 755-22, deberá ser igualmente considerado.

3.6. Ley Orgánica de las Fuerzas Armadas núm. 139-13

La Ley núm. 139-13 regula la organización, planificación, entrenamiento y operaciones de las Fuerzas Armadas y forma parte del marco institucional bajo el cual funcionan las unidades militares desplegadas en frontera.

3.7. Decretos núm. 325-06 y núm. 323-07

Estos instrumentos establecen la creación y responsabilidades operacionales de CESFRONT. La política mantendrá esas competencias y evitará crear estructuras paralelas que dupliquen su misión.

3.8. Ley núm. 12-21 de Desarrollo Fronterizo

La Ley núm. 12-21 crea la Zona Especial de Desarrollo Integral Fronterizo, abarcando:

a) Pedernales;

b) Independencia;

c) Elías Piña;

d) Dajabón;

e) Montecristi;

f) Santiago Rodríguez;

g) Bahoruco.

Su objetivo incluye promover inversión y desarrollo económico en esas provincias. La infraestructura tecnológica propuesta deberá utilizarse también para fortalecer la competitividad de esta zona.

3.9. Ley núm. 1-12 de Estrategia Nacional de Desarrollo 2030

La END contempla expresamente:

a) Fortalecer la presencia institucional del Estado en la frontera;

b) Fortalecer la capacidad productiva;

c) Promover la autosostenibilidad de las comunidades;

d) Fomentar el comercio fronterizo;

e) Crear infraestructura logística;

f) Proteger los ecosistemas fronterizos.

Por tanto, la presente política encuentra una alineación estratégica directa con la planificación nacional de largo plazo.

3.10. Protección de datos personales

La Ley núm. 172-13 complementará las garantías constitucionales relacionadas con el tratamiento de información personal. La utilización de biometría requerirá especialmente:

a) Finalidad determinada;

b) Seguridad reforzada;

c) Accesos autorizados;

d) Registro de consultas;

e) Plazos de conservación;

f) Protocolos de corrección;

g) Mecanismos de auditoría;

h) Régimen de responsabilidades.

La Ley núm. 172-13 reconoce como datos personales cualquier información concerniente a una persona física identificada o identificable.

3.11. Ciberseguridad y delitos tecnológicos

La infraestructura fronteriza inteligente deberá armonizarse con la Ley núm. 53-07 sobre Crímenes y Delitos de Alta Tecnología y demás normas nacionales de ciberseguridad.

El sistema será considerado infraestructura digital crítica y deberá diseñarse bajo criterios de defensa en profundidad.

3.12. Medio ambiente y salud

También deberán considerarse:

a) Ley núm. 64-00 General sobre Medio Ambiente y Recursos Naturales;

b) Ley núm. 42-01 General de Salud;

c) Normativa fitosanitaria y zoosanitaria;

d) Disposiciones sobre importación y circulación de alimentos, animales, vegetales y productos regulados.

3.13. Interoperabilidad gubernamental

Uno de los descubrimientos jurídicos y técnicos más importantes para esta propuesta es que el Estado dominicano **ya posee un marco oficial de interoperabilidad**.

La NORTIC A4:2024 establece directrices para que organismos gubernamentales intercambien información mediante la Plataforma Única de Interoperabilidad. Su última versión oficial disponible fue actualizada en junio de 2026.

Esto significa que nuestra propuesta no necesita inventar desde cero el mecanismo jurídico-técnico mediante el cual se conectarán las instituciones. Debe apoyarse en la infraestructura y estándares existentes.

3.14. Criterio jurídico general

La futura plataforma fronteriza deberá utilizar un modelo federado. Esto significa que cada institución conserva la propiedad, responsabilidad y autoridad sobre sus datos y competencias.

El sistema fronterizo únicamente solicitará, intercambiará y procesará las informaciones necesarias conforme a perfiles autorizados. La tecnología será la capa que conecte a todas las instituciones que intervengan en la frontera.

3.15. Reformas que deberán evaluarse posteriormente

Durante la elaboración del futuro anteproyecto se determinará si resulta necesario regular específicamente:

a) Tratamiento de biometría fronteriza;

b) Plazos de conservación de información;

c) Intercambio obligatorio de datos entre instituciones;

d) Evidencia digital producida por sensores y sistemas;

e) Sistemas automatizados de análisis de riesgo;

f) Auditoría electrónica de funcionarios;

g) Utilización operacional de sistemas no tripulados;

h) Responsabilidad por manipulación de registros;

i) Accesos indebidos;

j) Integridad de registros de frontera.

No se propondrá modificación legislativa alguna cuando las normas actualmente vigentes permitan resolver adecuadamente la materia.

CAPÍTULO IV

INVENTARIO DE INFRAESTRUCTURA Y TECNOLOGÍAS EXISTENTES

4.1. Principio de aprovechamiento de inversiones

La Política Nacional de Tecnificación Fronteriza no deberá sustituir indiscriminadamente los sistemas existentes. Su primera obligación será inventariar, evaluar, integrar y complementar.

Solo deberán adquirirse nuevas soluciones cuando las capacidades existentes resulten insuficientes, incompatibles u obsoletas.

4.2. Verja perimetral

La primera etapa contempló aproximadamente 54 kilómetros de verja física, acompañada de vías de comunicación, torres y puertas para patrullaje. La segunda fase incluye nuevas extensiones. En junio de 2025 comenzó la construcción de aproximadamente 13 kilómetros adicionales en Dajabón, incluyendo nuevas torres de vigilancia y accesos. El 5 de septiembre de 2026 comenzó otro tramo de 14.5 kilómetros en Jimaní. Estas obras deberán incorporarse desde su diseño al modelo tecnológico nacional.

4.3. Red de vigilancia

El proyecto fronterizo dominicano ya contempla importantes capacidades:

a) Fibra óptica;

b) Iluminación;

c) Cámaras diurnas;

d) Cámaras nocturnas;

e) Cámaras térmicas;

f) Sensores de movimiento;

g) Radares;

h) Torres de comunicaciones;

i) Drones;

j) Centros de mando C4;

k) Integración con el C5i.

En septiembre de 2025 se informó específicamente sobre 25 kilómetros de fibra óptica entre Manzanillo y Dajabón vinculados con cámaras térmicas, drones y sensores. La infraestructura existente constituye una base considerable para el sistema propuesto.

4.4. Centros de comando

Los centros de mando permiten convertir datos producidos por sensores en información operacional. La política propondrá posteriormente una arquitectura donde exista detección, clasificación, validación, alerta, despacho, respuesta, cierre del evento. Cada paso deberá quedar registrado electrónicamente.

4.5. Biometría migratoria

Durante 2026 la Dirección General de Migración fortaleció la capacitación para captura y validación mediante:

a) Reconocimiento facial;

b) Huellas dactilares;

c) Verificación de identidad.

Los esfuerzos se concentran en Dajabón, Pedernales, Elías Piña y Jimaní. También se han desarrollado procesos de biometrización asociados a mercados binacionales. Esto representa una de las piezas principales de la futura arquitectura de identidad fronteriza.

4.6. Identificación vehicular

El Proyecto IVF-RD desarrollado por Aduanas constituye otra pieza estratégica. Su diseño incluye:

a) Registro digital;

b) Tecnología RFID;

c) Códigos QR;

d) Holografía de seguridad;

e) Antenas lectoras;

f) Equipos especializados;

g) Plataforma de control;

h) Integración gubernamental.

A febrero de 2026, Aduanas reportaba un avance aproximado de 66 % en su primera fase y un presupuesto de RD$237,290,460, con horizonte de ejecución hasta mayo de 2027.

Consecuentemente, sería improcedente crear otro sistema nacional independiente de identificación vehicular fronteriza. La política deberá integrarse con IVF-RD.

4.7. Sistemas aduaneros

La Ley núm. 168-21 permite procedimientos electrónicos y Aduanas dispone de infraestructura digital destinada a gestionar importaciones, exportaciones y declaraciones.

La tecnificación fronteriza deberá conectarse con estos sistemas sin duplicarlos.

4.8. Infraestructura para biometrización

El POA de Migración para 2026 contempla infraestructura en Dajabón, Elías Piña, Pedernales y Jimaní destinada a biometrización y captura de datos relacionados con mercados binacionales. Estas instalaciones pueden constituir nodos iniciales del sistema integrado.

4.9. Cámaras corporales

La memoria institucional de Migración recoge infraestructura destinada al almacenamiento de videos producidos por cámaras corporales utilizadas en operaciones fronterizas.

Las bodycams presentan una oportunidad adicional para:

a) Protección del ciudadano;

b) Protección del funcionario;

c) Investigación administrativa;

d) Reconstrucción de incidentes;

e) Prevención de corrupción.

4.10. Infraestructura logística

El anuncio gubernamental de desarrollar puertos secos y centros logísticos fronterizos presenta una oportunidad para diseñar instalaciones que desde su origen incorporen:

a) Lectura automática de matrículas;

b) RFID;

c) Pesaje automatizado;

d) Rayos X cuando corresponda;

e) Videovigilancia;

f) Precintos electrónicos;

g) Control biométrico;

h) Gestión digital de turnos;

i) Trazabilidad de mercancías.

4.11. Infraestructura nacional de interoperabilidad

La OGTIC dispone de normas y plataformas destinadas al intercambio seguro de información gubernamental. La NORTIC A4:2024 deberá convertirse en referencia obligatoria para la arquitectura digital fronteriza.

4.12. Conclusión del inventario preliminar

El Estado dominicano ya posee una parte considerable de los elementos físicos y digitales necesarios. Por tanto, la inversión principal no debe concentrarse únicamente en comprar más tecnología. Debe priorizar:

a) Integración;

b) Cobertura;

c) Estandarización;

d) Interoperabilidad;

e) Redundancia;

f) Ciberseguridad;

g) Capacitación;

h) Mantenimiento;

i) Analítica;

j) Auditoría.

CAPÍTULO V

MODELO NACIONAL DE FRONTERA INTELIGENTE

5.1. Concepto

Se propone establecer el **Modelo Nacional de Frontera Inteligente de la República Dominicana**, sustentado tecnológicamente en un Sistema Integrado de Gestión Fronteriza Dominicana.

SIGFRO-RD

El SIGFRO-RD no constituirá una nueva institución pública. Será una **arquitectura tecnológica e interinstitucional** mediante la cual los organismos competentes podrán intercambiar información, coordinar operaciones y registrar actuaciones sin perder sus atribuciones legales.

5.2. Principio esencial

El sistema partirá de una regla fundamental: *"Un evento fronterizo, un registro digital trazable*."

Cuando ocurra un acontecimiento relevante en la frontera, el Estado deberá poder reconstruir posteriormente *qué ocurrió → dónde ocurrió → cuándo ocurrió → quién intervino → qué sistemas fueron consultados → qué decisión se tomó → quién la autorizó → cuál fue el resultado.*

5.3. Arquitectura general

SIGFRO-RD estará estructurado mediante diez capas principales.

Primera capa: infraestructura física

Comprenderá:

a) Verja;

b) Caminos de patrullaje;

c) Torres;

d) Puestos fronterizos;

e) Puertos secos;

f) Centros logísticos;

g) Centros de procesamiento;

h) Instalaciones operacionales.

Segunda capa: Sensores

Incluirá:

a) Cámaras;

b) Cámaras térmicas;

c) Sensores terrestres;

d) Detectores de movimiento;

e) Radares;

f) Lectores RFID;

g) Lectores de placas;

h) Sistemas de pesaje;

i) Drones;

j) Otros dispositivos autorizados.

Tercera capa: Identidad

Permitirá verificar legalmente:

a) Personas;

b) Funcionarios;

c) Vehículos;

d) Transportistas;

e) Comerciantes;

f) Operadores logísticos;

g) Empresas.

5.4. Identidad del funcionario

Todo funcionario que utilice SIGFRO-RD tendrá una identidad digital institucional individual. Quedará prohibido el uso de usuarios genéricos compartidos.

Cada operación deberá registrar automáticamente:

a) Funcionario;

b) Institución;

c) Fecha;

d) Hora;

e) Terminal;

f) Ubicación;

g) Consulta realizada;

h) Resultado;

i) Acción posterior.

Este mecanismo constituirá uno de los principales instrumentos anticorrupción del sistema.

5.5. Cuarta capa: Control migratorio

La información migratoria continuará bajo responsabilidad de la Dirección General de Migración.

SIGFRO-RD permitirá realizar las consultas necesarias para determinar, conforme a la ley, si una persona:

a) Se encuentra identificada;

b) Posee autorización correspondiente;

c) Presenta inconsistencias documentales;

d) Requiere verificación adicional;

e) Genera una alerta legalmente registrada.

5.6. Quinta capa: control vehicular

Se aprovechará prioritariamente IVF-RD. Cada vehículo autorizado podrá vincular:

matrícula + VIN + características + propietario/operador + RFID + fotografía + historial fronterizo autorizado.

Cuando un vehículo atraviese un punto equipado, su lectura podrá producir automáticamente un evento.

5.7. Sexta capa: mercancías

Cada carga formal deberá poder vincularse digitalmente con:

a) Declarante;

b) Transportista;

c) Vehículo;

d) Mercancía;

e) Cantidad;

f) Peso;

g) Documentos;

h) Procedencia;

i) Destino;

j) Inspección;

k) Liberación.

Esto permitirá desarrollar posteriormente mecanismos de trazabilidad comercial.

5.8. Séptima capa: Interoperabilidad

No se propone una base central que copie indiscriminadamente todas las bases gubernamentales. Se propone una arquitectura federada.

Ejemplo:

Cuando SIGFRO-RD necesite confirmar información vehicular, solicitará únicamente los datos autorizados a la fuente correspondiente. Cuando necesite información migratoria, consultará Migración.

Cuando requiera información aduanera, consultará Aduanas. Cuando corresponda verificar otras alertas legalmente autorizadas, consultará al organismo competente.

Esto permitirá aplicar el principio de: "La institución que genera el dato continúa siendo responsable del dato."

La arquitectura deberá cumplir la NORTIC A4:2024 y utilizar, cuando corresponda, la Plataforma Única de Interoperabilidad del Estado.

5.9. Octava capa: Inteligencia y análisis de riesgo

El sistema deberá analizar patrones.

Ejemplo:

Un vehículo cruza repetidamente en períodos extraordinariamente cortos. Esto no significa automáticamente que exista un delito.

Significa: ***el sistema incrementa el nivel de riesgo y recomienda verificación.***

La decisión coercitiva continuará correspondiendo al funcionario competente. La inteligencia artificial no sustituirá la autoridad legal.

5.10. Novena capa: Comando y respuesta

Cuando un sensor genere una alerta, SIGFRO-RD deberá:

a) Recibir el evento;

b) Determinar ubicación;

c) Incorporar cámaras disponibles;

d) Clasificar preliminarmente;

e) Remitir al centro correspondiente;

f) Asignar unidad;

g) Registrar salida;

h) Registrar llegada;

i) Documentar actuación;

j) Cerrar el evento.

Con ello podrá determinarse incluso el tiempo promedio de respuesta de las unidades.

5.11. Décima capa: Auditoría

Toda actuación relevante será auditable. El sistema deberá permitir determinar:

a) Quién consultó determinada información;

b) Quién modificó determinado registro;

c) Quién autorizó determinada operación;

d) Quién anuló una alerta;

e) Quién permitió un paso excepcional;

f) Qué fundamento fue registrado.

Una alerta nunca deberá desaparecer simplemente porque un funcionario decidió ignorarla. Podrá ser descartada legítimamente, pero deberá quedar constancia:

alerta → revisión → funcionario → fundamento → decisión.

5.12. Matriz de eventos fronterizos

Cada acontecimiento será clasificado inicialmente en categorías:

a) Persona;

b) Vehículo;

c) Mercancía;

d) Evento territorial;

e) Evento sanitario;

f) Evento ambiental;

g) Evento de seguridad;

h) Evento administrativo.

Un mismo acontecimiento podrá pertenecer a varias categorías.

5.13. Identificador único del evento

Cada evento generará un número único.

Ejemplo conceptual:

Esto permitirá reconstruir toda la actuación independientemente de la cantidad de instituciones participantes.

5.14. Correlación automatizada

Aquí reside una de las mayores ventajas del modelo.

Supongamos:

Persona A → vehículo B → comerciante C → carga D → múltiples cruces → horario E.

Observados individualmente podrían no resultar relevantes. SIGFRO-RD podrá detectar que forman parte de una misma secuencia operacional.

Este tipo de análisis deberá estar sujeto a reglas de legalidad, proporcionalidad y auditoría.

5.15. Modelo de vigilancia territorial

El territorio fronterizo podrá clasificarse dinámicamente:

Nivel 1 — Normal.	Sin patrones relevantes.
Nivel 2 — Atención.	Incremento de eventos o actividad inusual.
Nivel 3 — Alerta.	Patrón confirmado que requiere vigilancia reforzada.
Nivel 4 — Crítico.	Evento que demanda respuesta operacional inmediata.

Los niveles deberán actualizarse mediante información objetiva.

5.16. Patrullaje inteligente

En función del comportamiento histórico y de los eventos recientes, las unidades no serán desplegadas únicamente por recorridos rutinarios. El sistema podrá recomendar:

a) Horarios;

b) Rutas;

c) Zonas;

d) Frecuencias;

e) Recursos;

Esto permitirá transformar:

patrullaje uniforme → patrullaje basado en riesgo.

5.17. Continuidad operativa

La frontera inteligente no podrá quedar inutilizada debido a:

a) Apagón;

b) Corte de fibra;

c) Fallo de internet;

d) Daño de servidor;

e) Ataque cibernético.

Los puntos críticos deberán disponer de:

a) Energía redundante;

b) Conectividad redundante;

c) Operación degradada local;

d) Sincronización posterior;

e) Copias seguras;

f) Planes de contingencia.

5.18. Protección de datos por diseño

SIGFRO-RD deberá incorporar desde su construcción:

a) Acceso por roles;

b) Mínimo privilegio;

c) Cifrado;

d) Autenticación reforzada;

e) Registro inalterable de accesos;

f) Segregación de funciones;

g) Plazos de conservación;

h) Eliminación conforme a reglas;

i) Auditorías periódicas;

j) Protocolos ante incidentes.

5.19. Frontera física, digital y económica

El modelo final se apoyará en tres fronteras complementarias:

Frontera física	Define y protege el territorio.
Frontera digital	Permite detectar, identificar, registrar, analizar y responder.
Frontera económica	Organiza comercio, logística, inversión y empleo.

Ninguno de estos componentes debe desarrollarse aisladamente.

5.20. Resultado esperado

Al culminar la implementación, República Dominicana deberá disponer de una frontera donde pueda conocerse, dentro de los límites constitucionales y legales:

1. **Quién cruza;**
2. **Qué vehículo cruza;**
3. **Qué mercancía cruza;**
4. **Por dónde cruza;**
5. **Cuándo cruza;**
6. **Bajo qué autorización;**
7. **Qué funcionario intervino;**
8. **Qué controles se realizaron;**
9. **Qué alertas se produjeron;**
10. **Qué decisión fue adoptada.**

Ese será el fundamento operativo de la Frontera Inteligente de la República Dominicana.

CAPÍTULO VI

SISTEMA INTEGRADO DE GESTIÓN FRONTERIZA DOMINICANA — SIGFRO-RD

6.1. Definición

Se propone la creación funcional del **Sistema Integrado de Gestión Fronteriza Dominicana —SIGFRO-RD—**, entendido como la infraestructura tecnológica, operativa y de interoperabilidad destinada a conectar los sistemas de las instituciones que participan en la administración, vigilancia, seguridad, control migratorio, fiscalización aduanera y demás funciones legítimamente ejercidas en la frontera dominico-haitiana.

SIGFRO-RD no será concebido como una institución pública adicional ni asumirá competencias correspondientes a organismos existentes. Será una plataforma de coordinación tecnológica.

Su función fundamental será permitir que, ante un evento fronterizo, las instituciones competentes puedan intercambiar, consultar y correlacionar oportunamente la información que legalmente corresponda.

6.2. Principio de competencia institucional

La implementación de SIGFRO-RD estará sometida al principio de especialidad administrativa.

En consecuencia:

a) **Migración** continuará decidiendo los asuntos migratorios;

b) **Aduanas** continuará ejerciendo la autoridad aduanera;

c) **Ministerio de Defensa, Ejército y CESFRONT**, conforme a sus respectivas competencias, continuarán ejerciendo las funciones de seguridad y protección fronteriza;

d) **Ministerio Público y organismos de investigación** ejercerán sus competencias cuando existan indicios de infracción penal;

e) **Salud Pública** conservará sus competencias sanitarias;

f) **Agricultura y autoridades correspondientes** mantendrán las funciones fitosanitarias y zoosanitarias;

g) **Medio Ambiente** ejercerá sus competencias ambientales;

h) Las demás instituciones conservarán sus atribuciones conforme al ordenamiento jurídico.

Particular atención deberá prestarse a la Ley núm. 168-21, que establece la autoridad aduanera en la Zona Primaria Aduanera y simultáneamente contempla mecanismos de colaboración con otros organismos del Estado. La misma legislación incorpora formalmente la gestión de riesgo mediante herramientas electrónicas y utilización sistemática de información.

6.3. Gobernanza funcional

Se propone establecer mediante el instrumento jurídico correspondiente un **Comité Técnico Interinstitucional de SIGFRO-RD**, sin personalidad jurídica ni estructura administrativa independiente.

Este comité tendrá funciones exclusivamente técnicas de coordinación.

Participarán permanentemente:

a) Ministerio de Defensa;

b) CESFRONT;

c) Dirección General de Migración;

d) Dirección General de Aduanas;

e) OGTIC;

f) Organismos nacionales competentes en ciberseguridad;

g) Otras instituciones cuya participación sea necesaria según las materias tratadas.

La participación de una institución en SIGFRO-RD no implicará transferencia de competencias.

6.4. Autoridad según el tipo de evento

En lugar de establecer una autoridad única para cualquier acontecimiento fronterizo, SIGFRO-RD utilizará el concepto de **autoridad funcional del evento**.

Por ejemplo:

Evento	**Autoridad funcional principal**
Entrada o salida migratoria	Dirección General de Migración
Declaración, inspección o liberación	Dirección General de Aduanas

Evento	Autoridad funcional principal
de mercancía	
Cruce irregular fuera de punto autorizado	Autoridad de seguridad fronteriza competente
Tráfico ilícito o delito	Autoridades investigativas y Ministerio Público según corresponda
Alerta sanitaria	Ministerio de Salud Pública
Riesgo animal o vegetal	Autoridad agropecuaria competente
Delito ambiental	Ministerio de Medio Ambiente y autoridades correspondientes

De esta manera se evita que la plataforma tecnológica altere las competencias establecidas por ley.

6.5. Arquitectura Federada

SIGFRO-RD deberá desarrollarse bajo una arquitectura federada. Esto significa que no será necesario trasladar indiscriminadamente toda la información gubernamental hacia una gigantesca base fronteriza.

Cada institución conservará sus sistemas. La plataforma solicitará únicamente la información estrictamente necesaria para realizar una operación determinada.

Ejemplo:

SIGFRO-RD → consulta → institución responsable → respuesta autorizada → registro de consulta.

La NORTIC A4:2024 ya establece estándares oficiales de interoperabilidad jurídica, organizacional, semántica y técnica, y reconoce la Plataforma Única de Interoperabilidad como mecanismo oficial para el intercambio de información gubernamental. Su última versión publicada por OGTIC fue actualizada el 23 de junio de 2026.

Por consiguiente, SIGFRO-RD deberá construirse sobre este marco y no crear innecesariamente una infraestructura paralela.

6.6. Identificador Único de Evento Fronterizo

Cada acontecimiento registrado en la plataforma generará un **Identificador Único de Evento Fronterizo —IUEF—**.

Podrá utilizar una estructura equivalente a **FR-2027-DAJ-000000125.**

El identificador permitirá relacionar:

a) Persona;

b) Vehículo;

c) Mercancía;

d) Lugar;

e) Fecha;

f) Funcionarios intervinientes;

g) Cámaras relacionadas;

h) Inspecciones;

i) Alertas;

j) Decisiones;

k) Documentos;

l) Resultado final.

6.7. Expediente digital del evento

Cada evento podrá generar automáticamente un expediente electrónico. Este expediente no sustituirá los expedientes administrativos o judiciales exigidos por la legislación. Funcionará como registro operacional.

Deberá indicar:

a) Fecha y hora de apertura;

b) Punto fronterizo o coordenada;

c) Institución que originó el evento;

d) Tipo de evento;

e) Nivel inicial de riesgo;

f) Información consultada;

g) Alertas generadas;

h) Funcionarios participantes;

i) Actuaciones realizadas;

j) Evidencias asociadas;

k) Decisión adoptada;

l) Fecha y hora de cierre.

6.8. Registro de actuación del funcionario

Todo acceso a SIGFRO-RD será individual. Quedará prohibido compartir usuarios y contraseñas. Cada interacción relevante deberá producir automáticamente un registro que indique:

quién → hizo qué → sobre qué registro → cuándo → desde dónde → con qué resultado.

La trazabilidad deberá abarcar igualmente a supervisores y administradores tecnológicos.

6.9. Autenticación reforzada

Dependiendo del nivel de acceso, deberá exigirse:

a) Credencial institucional;

b) Contraseña;

c) Segundo factor de autenticación;

d) Certificado digital cuando corresponda;

e) Autenticación biométrica para operaciones particularmente sensibles cuando exista fundamento legal;

f) Equipo institucional previamente autorizado.

6.10. Principio del mínimo privilegio

Ningún funcionario deberá disponer automáticamente de acceso completo a la plataforma.

Ejemplo:

Un inspector migratorio no necesitará visualizar información fiscal completa de una empresa. Un funcionario aduanero no necesitará acceder indiscriminadamente a expedientes migratorios. Un operador de cámaras no tendrá necesariamente acceso a información tributaria.

Cada usuario visualizará únicamente la información indispensable para cumplir sus funciones.

6.11. Intercambio de alertas

Las instituciones podrán publicar en SIGFRO-RD determinados tipos de alertas legalmente autorizadas. Una alerta deberá contener, como mínimo:

a) Institución originadora;

b) Fecha;

c) Base o fundamento;

d) Nivel de prioridad;

e) Vigencia;

f) Acción requerida;

g) Restricción de acceso;

h) Responsable institucional.

Las alertas vencidas deberán desactivarse conforme a las reglas establecidas.

6.12. Prohibición de alertas anónimas dentro del sistema

Ningún funcionario podrá introducir una alerta operacional sin identificación de su origen. Esto no impide la existencia de sistemas externos de denuncias ciudadanas anónimas. Sin embargo, cuando una denuncia produzca una alerta oficial en SIGFRO-RD, deberá quedar identificado el funcionario o unidad que decidió formalizarla.

6.13. Modificación y eliminación de registros

Los registros operacionales relevantes no deberán poder eliminarse directamente por usuarios ordinarios.

Las correcciones deberán realizarse mediante:

registro original → corrección → motivo → funcionario → fecha.

Nunca:

registro original → borrado sin evidencia.

6.14. Motor de reglas

SIGFRO-RD incorporará un motor configurable de reglas.

Ejemplos:

a) Vehículo con identificador alterado;

b) Número inusual de cruces;

c) Documento vencido;

d) Diferencia significativa entre peso declarado y medido;

e) Precinto electrónico vulnerado;

f) Mercancía que requiere autorización especial;

g) Matrícula asociada a alerta;

h) Evento detectado fuera de un paso autorizado.

Las reglas deberán ser revisadas periódicamente.

6.15. Inteligencia artificial

Los algoritmos de inteligencia artificial podrán utilizarse para:

a) Detección de patrones;

b) Reconocimiento de objetos;

c) Correlación de eventos;

d) Priorización de alertas;

e) Predicción logística;

f) Detección de anomalías;

g) Optimización de patrullaje.

Pero se establecerá una regla fundamental:

Ninguna decisión restrictiva de derechos podrá fundamentarse exclusivamente en una decisión automática.

Una alerta algorítmica deberá ser evaluada por la autoridad competente.

6.16. Operación desconectada

Los puntos fronterizos deberán conservar capacidades mínimas cuando se interrumpa la conectividad. El sistema podrá operar temporalmente mediante procedimientos degradados que permitan:

a) Registrar actuaciones localmente;

b) Mantener listas críticas actualizadas;

c) Continuar determinadas operaciones;

d) Sincronizar posteriormente los registros;

e) Detectar posibles conflictos producidos durante la desconexión.

6.17. Alta disponibilidad

Los sistemas críticos deberán diseñarse para operar permanentemente. Deberán disponer de:

a) Servidores redundantes;

b) Comunicaciones redundantes;

c) Energía de respaldo;

d) Copias de seguridad;

e) Centros alternativos;

f) Recuperación ante desastres;

g) Monitoreo permanente.

6.18. Protección de datos

SIGFRO-RD deberá incorporar las medidas técnicas y organizativas necesarias para impedir alteración, pérdida, tratamiento o acceso no autorizado a datos personales, en consonancia con los principios de seguridad establecidos en la Ley núm. 172-13.

6.19. Auditoría periódica

El sistema deberá someterse a:

a) Auditorías de seguridad;

b) Auditorías de acceso;

c) Auditorías de integridad de datos;

d) Pruebas de penetración;

e) Evaluaciones de vulnerabilidad;

f) Auditorías de algoritmos;

g) Evaluaciones de cumplimiento jurídico.

6.20. Resultado esperado

SIGFRO-RD deberá convertir múltiples actuaciones gubernamentales independientes en una cadena institucional digitalmente coordinada, sin alterar la competencia jurídica de ninguna institución.

CAPÍTULO VII

IDENTIFICACIÓN BIOMÉTRICA Y CONTROL MIGRATORIO

7.1. Objetivo

El componente biométrico tendrá como propósito incrementar la capacidad de la Dirección General de Migración para determinar de manera confiable la identidad de las personas sometidas legítimamente a control migratorio.

La Dirección General de Migración ya está fortaleciendo durante 2026 sus capacidades de reconocimiento facial, huellas dactilares y validación de identidad en Dajabón, Pedernales, Elías Piña y Jimaní. Igualmente ha desarrollado procesos de biometrización relacionados con el acceso a mercados binacionales.

Por tanto, esta política **no propone sustituir ese sistema**, sino fortalecerlo e integrarlo.

7.2. Autoridad competente

Toda actuación migratoria derivada del sistema permanecerá bajo responsabilidad de la Dirección General de Migración y dentro de las competencias establecidas en la Ley núm. 285-04 y su Reglamento de Aplicación núm. 631-11. El propio reglamento define las responsabilidades institucionales vinculadas con la regulación de los flujos migratorios.

7.3. Biometría como instrumento de identidad

La biometría deberá utilizarse principalmente para responder una pregunta:

"¿Es esta persona quien afirma ser?"

La plataforma podrá incorporar, conforme al fundamento jurídico aplicable:

a) Huellas dactilares;

b) Reconocimiento facial;

c) Fotografía digital;

d) Otras tecnologías biométricas cuya utilización sea legalmente autorizada.

7.4. Verificación e identificación

Se distinguirán técnicamente dos operaciones:

Verificación 1:1.

La persona presenta una identidad y el sistema comprueba si la biometría coincide.

Identificación 1:N.

La biometría es comparada contra múltiples registros para determinar una posible identidad.

La segunda modalidad presenta mayores implicaciones para la privacidad y deberá contar con mayores controles, justificación y auditoría.

7.5. Registro Fronterizo de Movilidad Autorizada

Se podrá desarrollar dentro de Migración un módulo destinado a las personas cuya modalidad legal de tránsito fronterizo requiera identificaciones frecuentes.

El sistema no creará por sí mismo ninguna categoría migratoria.

Su función será únicamente administrar tecnológicamente las modalidades que estén reconocidas por legislación, reglamentación o autorización competente.

7.6. Registro de comerciantes fronterizos

Cuando la legislación permita mecanismos especiales relacionados con mercados binacionales o actividades fronterizas, podrá establecerse un registro digital que vincule:

a) Identidad;

b) Fotografía;

c) Biometría autorizada;

d) Actividad declarada;

e) Punto fronterizo autorizado;

f) Vigencia;

g) Historial de movimientos permitido;

h) Restricciones aplicables.

7.7. Credencial fronteriza

Cuando resulte jurídicamente procedente, determinados usuarios recurrentes podrán recibir una credencial física o digital.

Esta credencial podrá incorporar:

a) Código QR seguro;

b) Identificador único;

c) Fotografía;

d) Elementos antifalsificación;

e) Vigencia;

f) Información mínima de categoría.

La credencial no sustituirá pasaporte, visa, permiso ni documento migratorio cuando estos sean legalmente exigibles.

7.8. Captura inicial

La captura biométrica deberá realizarse mediante equipos certificados y procedimientos estandarizados.

Se registrará:

a) Fecha;

b) Punto;

c) Equipo utilizado;

d) Operador;

e) Calidad de captura;

f) Documentos presentados;

g) Resultado.

7.9. Calidad biométrica

El sistema deberá impedir que registros biométricos deficientes produzcan falsas coincidencias.

Se establecerán estándares mínimos de:

a) Resolución;

b) Calidad de huellas;

c) Iluminación facial;

d) Posición;

e) Detección de vida;

f) Integridad del archivo.

7.10. Detección de vida

Los dispositivos biométricos deberán incorporar progresivamente mecanismos que permitan detectar intentos de suplantación mediante:

a) Fotografías;

b) Videos;

c) Moldes de huellas;

d) Máscaras;

e) Otros mecanismos de presentación fraudulenta.

7.11. Resultado inconcluso

Cuando la tecnología no pueda identificar confiablemente a una persona ***el sistema no presumirá automáticamente irregularidad*.** La persona será remitida a verificación secundaria. Esto resulta particularmente importante frente a:

a) Huellas deterioradas;

b) Personas de edad avanzada;

c) Lesiones;

d) Problemas del dispositivo;

e) Cambios físicos;

f) Baja calidad de captura.

7.12. Verificación documental

Biometría y documentación deberán funcionar conjuntamente. El proceso podrá incluir:

documento → validación → biometría → consulta migratoria → decisión.

7.13. Detección de duplicidades

La plataforma podrá detectar casos en que una misma biometría aparezca asociada a identidades diferentes. El resultado deberá producir una alerta de verificación y no una conclusión automática de fraude.

7.14. Mercados binacionales

Los mercados binacionales presentan condiciones particulares debido a la entrada y salida recurrente de personas en períodos cortos. El sistema podrá permitir:

a) Registro previo;

b) Captura biométrica;

c) Carriles diferenciados;

d) Control automático de acceso;

e) Registro de entrada;

f) Registro de salida;

g) Alertas por incumplimiento de las condiciones autorizadas.

Migración informó en mayo de 2026 que estaba verificando precisamente los procesos de biometrización y control de acceso de personas que entran y salen el mismo día en zonas de actividad comercial fronteriza.

7.15. Control de entrada y salida

Un principio operacional importante será:

Entrada registrada debe corresponder, cuando corresponda, con salida registrada.

Esto permitirá identificar registros incompletos y mejorar las estadísticas migratorias.

7.16. Interoperabilidad

Migración podrá recibir consultas de otras instituciones a través de SIGFRO-RD únicamente dentro de los límites legalmente autorizados. No será necesario exponer todo el expediente migratorio.

Ejemplo de respuesta:

Identidad validada: Sí.

Documento vigente: Sí.

Alerta aplicable: No

En muchas situaciones no será necesario proporcionar información adicional.

7.17. Protección especial de datos biométricos

La información biométrica requerirá un régimen de seguridad reforzado. Deberá contemplarse:

a) Cifrado;

b) Separación lógica;

c) Accesos restringidos;

d) Trazabilidad completa;

e) Prohibición de copias locales no autorizadas;

f) Auditoría;

g) Gestión de incidentes;

h) Conservación conforme al fundamento legal aplicable.

7.18. Prohibición de uso secundario indiscriminado

Los registros biométricos obtenidos para control fronterizo no deberán utilizarse automáticamente para finalidades completamente diferentes. Cualquier utilización adicional deberá contar con fundamento jurídico.

7.19. Reconocimiento facial

Cuando se utilice reconocimiento facial, deberá implementarse un sistema de evaluación humana ante coincidencias relevantes. La respuesta tecnológica deberá expresarse como: **posible coincidencia → verificar.**

Nunca como: **identidad culpable → actuar automáticamente.**

7.20. Indicadores

Migración podrá evaluar:

a) Tiempo promedio de procesamiento;

b) Porcentaje de verificaciones exitosas;

c) Tasa de revisión secundaria;

d) Duplicidades detectadas;

e) Errores biométricos;

f) Equipos fuera de servicio;

g) Tiempo de resolución de incidencias;

h) Entradas sin salida correspondiente cuando resulte aplicable.

CAPÍTULO VIII

ADUANA INTELIGENTE Y TRAZABILIDAD DE MERCANCÍAS

8.1. Objetivo

El propósito de la Aduana Inteligente Fronteriza será incrementar simultáneamente control, trazabilidad, seguridad, facilitación del comercio legítimo. La tecnificación no deberá convertir la frontera en un obstáculo innecesario para el comercio formal. Debe lograr exactamente lo contrario más control sobre el riesgo y menos fricción para las operaciones de bajo riesgo.

8.2. Base legal

La Ley núm. 168-21 introdujo herramientas especialmente compatibles con este modelo, incluyendo:

a) Gestión de riesgo;

b) Herramientas electrónicas;

c) Controles no intrusivos;

d) Tecnologías de información;

e) Firma electrónica o digital;

f) Coordinación con órganos para-aduaneros;

g) Procedimientos aduaneros modernizados.

Asimismo, Aduanas utiliza la Declaración Única Aduanera electrónica mediante SIGA.

Por consiguiente, SIGFRO-RD deberá integrarse con SIGA y demás plataformas existentes, no reemplazarlas.

8.3. Principio de información anticipada

Siempre que el régimen correspondiente lo permita, la información relacionada con una operación deberá estar disponible antes de que el vehículo llegue físicamente al punto de inspección. Esto permitirá preparar previamente:

a) Perfil de riesgo;

b) Documentación;

c) Autorizaciones;

d) Inspecciones requeridas;

e) Disponibilidad de organismos especializados.

8.4. Identificador Único de Carga

Cada operación relevante podrá recibir un identificador vinculado a:

a) Declarante;

b) Exportador o importador;

c) Transportista;

d) Conductor;

e) Vehículo;

f) Remolque;

g) Mercancía;

h) Peso;

i) Documentos;

j) Procedencia;

k) Destino;

l) Declaración aduanera.

8.5. Flujo digital

El modelo general podrá funcionar:

Registro→ validación documental→ análisis de riesgo→ llegada→ identificación vehicular→ pesaje → inspección requerida → autorización → salida → cierre.

8.6. Sistema de citas para carga

Para determinados tipos de operaciones podrá incorporarse un sistema de programación que permita distribuir la llegada de vehículos. Esto podría:

a) Reducir congestionamientos;

b) Evitar filas prolongadas;

c) Distribuir personal;

d) Programar inspecciones;

e) Incrementar seguridad;

f) Mejorar la capacidad logística.

8.7. Pesaje automatizado

Los puntos principales podrán disponer de básculas integradas digitalmente. El peso deberá incorporarse automáticamente al evento. Esto permitirá comparar peso declarado vs. peso registrado. Diferencias por encima de parámetros razonables podrán producir una alerta.

8.8. Inspección no intrusiva

Cuando el tipo, volumen y nivel de riesgo lo justifique, deberán utilizarse tecnologías de inspección no intrusiva compatibles con la Ley núm. 168-21.

Las imágenes producidas deberán vincularse automáticamente con el evento correspondiente.

8.9. Precintos electrónicos

Para cargas sometidas a regímenes que requieran seguimiento especial podrá evaluarse el uso de precintos electrónicos. El dispositivo podrá registrar:

a) Número;

b) Fecha de colocación;

c) Funcionario;

d) Vehículo;

e) Carga;

f) Estado;

g) Apertura autorizada;

h) Manipulación irregular.

8.10. Cadena de trazabilidad

El sistema deberá poder reconstruir:

mercancía → declaración → empresa → conductor → vehículo → inspección → funcionario → liberación → salida.

Esta cadena tendrá especial relevancia para investigaciones posteriores.

8.11. Gestión de riesgo

La Ley núm. 168-21 reconoce expresamente el análisis de riesgo y el uso de herramientas electrónicas para los controles aduaneros. SIGFRO-RD deberá fortalecer esos mecanismos mediante información adicional procedente del entorno fronterizo. El análisis podrá considerar, conforme a las reglas de Aduanas:

a) Historial del operador;

b) Tipo de mercancía;

c) Valor;

d) Peso;

e) Frecuencia;

f) Ruta;

g) Vehículo;

h) Inconsistencias documentales;

i) Alertas legalmente autorizadas.

8.12. Selección de inspección

Cuando corresponda una inspección física, el sistema podrá asignarla electrónicamente.

Esto reducirá la posibilidad de que un operador seleccione deliberadamente siempre al mismo inspector.

8.13. Redistribución aleatoria

Cuando resulte operativamente conveniente, la plataforma podrá distribuir determinados expedientes entre inspectores siguiendo criterios:

a) Disponibilidad;

b) Especialización;

c) Carga de trabajo;

d) Aleatoriedad controlada.

El supervisor podrá modificar la asignación, pero deberá justificarlo electrónicamente.

8.14. Organismos para-aduaneros

Las mercancías sujetas a controles adicionales podrán activar automáticamente intervenciones de:

a) Agricultura;

b) Salud Pública;

c) Medio Ambiente;

d) Autoridades sanitarias;

e) Otras autoridades legalmente competentes.

La Ley núm. 168-21 contempla precisamente la coordinación de las labores de órganos para-aduaneros con la Aduana.

8.15. Ventanilla operacional

El operador no deberá tener que presentar repetidamente la misma documentación ante múltiples organismos cuando legal y técnicamente sea posible compartirla. La regla será: *"El Estado no debe solicitar nuevamente un dato válido que ya posee y está legalmente autorizado a reutilizar."*

8.16. Comercio fronterizo de pequeña escala

Deberá estudiarse un mecanismo simplificado de formalización para pequeños comerciantes recurrentes. Este mecanismo tendría que establecerse mediante la

legislación o regulación correspondiente y no deberá utilizarse para evadir controles aduaneros. Podría permitir:

a) Registro simplificado;

b) Identificación del comerciante;

c) Declaraciones digitales sencillas;

d) Historial de operaciones;

e) Límites cuando legalmente correspondan;

f) Educación tributaria y aduanera.

8.17. Operadores confiables

Los mecanismos de facilitación podrán aprovechar programas ya establecidos por Aduanas, incluyendo la lógica del Operador Económico Autorizado.

Los operadores con buen historial y bajo riesgo podrían beneficiarse de procedimientos más ágiles dentro de los límites legales.

8.18. Auditoría posterior

Una carga liberada no desaparecerá del sistema. Los datos permanecerán disponibles conforme a los plazos legales correspondientes para:

a) Auditoría;

b) Fiscalización;

c) Investigación;

d) Estadística;

e) Análisis de patrones.

8.19. Prevención de corrupción

El sistema deberá permitir detectar patrones tales como:

a) Inspector que libera cantidades anormales de operaciones;

b) Anulaciones recurrentes de alertas;

c) Operador que siempre utiliza el mismo funcionario;

d) Cambios frecuentes de peso;

e) Modificaciones posteriores a inspecciones;

f) Liberaciones fuera de parámetros habituales.

Estos patrones producirán revisiones administrativas, no presunciones automáticas de culpabilidad.

8.20. Objetivo final

La Aduana Inteligente deberá lograr que la carga legítima se mueva más rápido y la carga riesgosa sea examinada con mayor precisión.

CAPÍTULO IX

IDENTIFICACIÓN Y CONTROL VEHICULAR FRONTERIZO

9.1. Punto de partida

La República Dominicana ya desarrolla una herramienta particularmente importante para esta propuesta el Proyecto de Identificación Vehicular Fronteriza —IVF-RD—. A febrero de 2026, su primera fase reportaba un avance de aproximadamente 66 %, con ejecución prevista hasta mayo de 2027 y presupuesto de RD$237,290,460. El proyecto incorpora RFID, códigos QR, holografía, plataforma digital y equipos especializados.

La memoria institucional de Aduanas explica que la etiqueta RFID es instalada en el parabrisas y que antenas ubicadas en los puntos de control permiten registrar automáticamente los movimientos vehiculares. Por ello *SIGFRO-RD no creará un sistema competidor de IVF-RD, l*o integrará.

9.2. Identidad digital del vehículo

Cada vehículo que participe en operaciones fronterizas sometidas al régimen correspondiente deberá disponer de una identidad digital verificable. Esta identidad podrá relacionar:

a) Matrícula;

b) VIN o chasis;

c) Marca;

d) Modelo;

e) Año;

f) Tipo;

g) Color;

h) Propietario registrado;

i) Operador autorizado;

j) Identificador IVF-RD;

k) Fotografía;

l) Historial fronterizo legalmente disponible.

9.3. Principio de múltiples factores vehiculares

Nunca deberá dependerse exclusivamente de una placa o etiqueta. La identificación deberá poder combinar matrícula + RFID + VIN + características físicas + imagen. De esta forma, copiar una matrícula no será suficiente para suplantar un vehículo.

9.4. Lectura automática

Los puntos de control podrán incorporar:

a) Lectores RFID;

b) Reconocimiento automático de matrículas;

c) Cámaras;

d) Lectores QR;

e) Básculas;

f) Detectores de altura;

g) Conteo de ejes;

h) Otros sensores técnicamente justificables.

9.5. Secuencia de llegada

Al aproximarse un vehículo RFID detectado → matrícula reconocida → fotografía → consulta → validación → riesgo → carril correspondiente.

Gran parte de la información podrá verificarse antes de que el conductor llegue a la caseta.

9.6. RFID como identificador y no como título

La etiqueta RFID no constituirá prueba de propiedad. Será un mecanismo técnico para identificar el vehículo dentro del sistema.

La propiedad continuará determinada por los registros legalmente correspondientes.

9.7. Registro nacional vehicular

Cuando exista habilitación jurídica y técnica, SIGFRO-RD podrá consultar los registros nacionales pertinentes para verificar:

a) Existencia del vehículo;

b) Matrícula;

c) VIN;

d) Características;

e) Propietario registrado;

f) Otras condiciones legalmente consultables.

9.8. Vehículos con alerta

Cuando exista una alerta legalmente válida relacionada con un vehículo, la lectura automática deberá mostrar:

a) Institución emisora;

b) Tipo de alerta;

c) Vigencia;

d) Acción requerida.

El funcionario no deberá visualizar necesariamente toda la investigación relacionada.

9.9. Vehículos extranjeros

Los vehículos extranjeros sometidos a regímenes de admisión o circulación temporal deberán recibir los identificadores que correspondan conforme al régimen aduanero aplicable. Podrá utilizarse un identificador fronterizo temporal que relacione:

a) Matrícula extranjera;

b) VIN;

c) Propietario o responsable;

d) Conductor;

e) Fecha de ingreso;

f) Régimen;

g) Fecha límite cuando corresponda;

h) Punto de entrada;

i) Salida registrada.

9.10. Motocicletas

El modelo deberá incorporar también las motocicletas.

Deberán estudiarse soluciones adecuadas debido a que los sistemas de identificación diseñados para parabrisas no siempre son aplicables.

9.11. Remolques y contenedores

En transporte de carga deberán distinguirse:

1. Cabezal
2. Remolque
3. Contenedor
4. Carga.

Cada componente podrá poseer identificación independiente. Esto permitirá detectar sustituciones.

9.12. Fotografía automática

Cada cruce relevante podrá producir imágenes del vehículo desde diferentes ángulos. Estas imágenes podrán ayudar a detectar cambio de color, matrícula diferente, remolque distinto, daños, modificaciones físicas, sustitución de componentes.

9.13. Detección de anomalías

El sistema podrá generar alertas por:

a) RFID correspondiente a otra matrícula;

b) Matrícula no correspondiente al VIN registrado;

c) Etiqueta duplicada;

d) Cruces físicamente incompatibles;

e) Exceso inusual de frecuencia;

f) Cambio constante de conductor;

g) Entrada sin salida cuando el régimen lo exija;

h) Vehículo temporal que exceda plazo autorizado.

9.14. Cruces frecuentes

Un elevado número de cruces no será considerado automáticamente irregular. Podrá tratarse de:

a) Transportista;

b) Comerciante;

c) Operador logístico;

d) Trabajador autorizado.

El sistema evaluará el comportamiento dentro del contexto correspondiente.

9.15. Alteración de etiquetas

Las etiquetas de identificación deberán disponer de mecanismos contra:

a) Traslado entre vehículos;

b) Reproducción;

c) Manipulación;

d) Falsificación.

IVF-RD ya contempla elementos como RFID, códigos QR y holografía, lo que proporciona una base tecnológica sólida.

9.16. Excepciones

Deberá existir un procedimiento para:

a) RFID dañado;

b) Matrícula ilegible;

c) Vehículo de emergencia;

d) Fallo del lector;

e) Vehículo autorizado que todavía no disponga de etiqueta;

f) Contingencias.

Toda excepción deberá registrarse.

9.17. Revisión manual

Cuando el sistema no pueda verificar automáticamente un vehículo se remitirá a inspección secundaria. No deberá permitirse que un operador simplemente ignore el error y continúe el proceso ordinario.

9.18. Integración con mercancías

Cuando un vehículo transporte carga *vehículo + conductor + declaración + carga + remolque + inspección,* deberán quedar vinculados dentro del mismo evento.

9.19. Protección frente a vigilancia excesiva

La utilización de RFID y lectura automática estará dirigida al control fronterizo y demás finalidades legalmente establecidas.

No deberá utilizarse el sistema fronterizo para seguimiento general e indiscriminado de vehículos fuera de ese ámbito sin fundamento legal.

9.20. Indicadores

Entre los indicadores podrán incluirse:

a) Vehículos procesados;

b) Tiempo promedio;

c) Lecturas automáticas exitosas;

d) Etiquetas alteradas;

e) Duplicidades;

f) Inspecciones secundarias;

g) Fallas técnicas;

h) Vehículos temporales sin salida registrada;

i) Alertas confirmadas;

j) Falsos positivos.

CAPÍTULO X

VIGILANCIA ELECTRÓNICA, SENSORES, RADARES Y CÁMARAS

10.1. Concepto

La vigilancia tecnológica deberá extender la capacidad del Estado para observar la frontera más allá de los lugares donde pueda existir presencia física permanente.

La lógica será "Detectar antes de interceptar." Los militares y demás unidades fronterizas deberán recibir información suficientemente temprana para decidir dónde concentrar sus recursos.

10.2. Infraestructura existente

República Dominicana ya ha iniciado un despliegue considerable.

La segunda etapa de la verja incorporó 25 kilómetros de fibra óptica entre Manzanillo y Dajabón conectados con cámaras térmicas, drones y sensores de movimiento.

El modelo fronterizo existente contempla igualmente cámaras diurnas y nocturnas, radares terrestres y marítimos, torres, unidades aéreas no tripuladas y centros C4 integrados con el C5i.

En 2026 el Ministerio de Defensa reportó también la utilización de cámaras, fibra óptica, radiofrecuencia y drones autónomos supervisados desde el C5i.

Por tanto, este capítulo propone principalmente integrar, ampliar y normalizar dichas capacidades.

10.3. Red Integrada de Sensores Fronterizos

Se propone estructurar una Red Integrada de Sensores Fronterizos —RISF— como componente de SIGFRO-RD. Esta red podrá integrar:

a) Cámaras convencionales;

b) Cámaras térmicas;

c) Cámaras de baja luminosidad;

d) Sensores de movimiento;

e) Sensores terrestres;

f) Radares terrestres;

g) Radares marítimos donde corresponda;

h) Drones;

i) Sistemas acústicos técnicamente justificables;

j) Otros dispositivos autorizados.

10.4. Georreferenciación

Cada dispositivo deberá disponer de posición geográfica registrada. Cuando produzca una alerta, el centro de mando conocerá inmediatamente:

a) Sensor;

b) Ubicación;

c) Hora;

d) Tipo de evento;

e) Dispositivos cercanos;

f) Unidad operacional más próxima.

10.5. Fusión de sensores

Uno de los elementos más importantes será la combinación de múltiples fuentes.

Ejemplo:

Sensor terrestre detecta movimiento/Cámara térmica confirma presencia/Sistema clasifica posible grupo de personas/Dron es enviado a verificar/Centro de mando confirma/Unidad terrestre recibe coordenadas.

Este proceso aumenta significativamente la certeza antes de desplegar personal.

10.6. Clasificación automatizada

Las cámaras podrán utilizar analítica para distinguir inicialmente:

a) Persona;

b) Grupo de personas;

c) Vehículo;

d) Motocicleta;

e) Animal;

f) Objeto;

g) Movimiento ambiental.

La clasificación automática permitirá reducir falsas alarmas.

10.7. Regla de confirmación

Cuando sea operacionalmente posible, determinadas alertas deberán ser verificadas mediante un segundo sensor antes de movilizar recursos. Por ejemplo:

movimiento + cámara = mayor certeza.

Sin embargo, eventos críticos podrán requerir respuesta inmediata.

10.8. Cámaras térmicas

Las cámaras térmicas serán especialmente útiles durante:

a) Horas nocturnas;

b) Condiciones de baja visibilidad;

c) Zonas sin iluminación;

d) Áreas rurales;

e) Seguimiento de movimientos.

10.9. Radares

Los radares podrán utilizarse para detectar desplazamientos en áreas donde una cámara convencional tenga limitaciones. En zonas costeras o lacustres podrán integrarse tecnologías apropiadas para controlar movimientos marítimos o acuáticos cuando corresponda.

10.10. Torres inteligentes

Las torres fronterizas podrán convertirse progresivamente en nodos multisensor. Una torre podría integrar:

a) Cámara panorámica;

b) Cámara térmica;

c) Radio;

d) Antenas;

e) Sensor meteorológico;

f) Iluminación;

g) Comunicaciones;

h) Sistema eléctrico autónomo.

10.11. Zonas tecnológicas

La frontera no necesita disponer exactamente de la misma densidad tecnológica en cada kilómetro. La infraestructura deberá asignarse según riesgo. Podrán definirse:

Zona tecnológica A — Alta criticidad	Mayor densidad de sensores y vigilancia permanente.
Zona tecnológica B — Riesgo medio	Cobertura combinada fija y móvil.
Zona tecnológica C — Bajo riesgo	Vigilancia periódica y sistemas móviles.

Esta clasificación podrá variar con el tiempo.

10.12. Mapa dinámico de riesgo

SIGFRO-RD deberá producir un mapa actualizado mediante:

a) Eventos históricos;

b) Incidentes recientes;

c) Alertas;

d) Movimientos detectados;

e) Información operacional;

f) Condiciones geográficas;

g) Variables temporalmente relevantes.

No deberán hacerse públicas aquellas capas cuya divulgación comprometa operaciones de seguridad.

10.13. Patrullaje basado en evidencia

Las rutas de patrullaje podrán ajustarse en función de:

a) Horario;

b) Día;

c) Sector;

d) Frecuencia histórica;

e) Alertas;

f) Eventos recientes.

De esta forma, los patrones de patrullaje no serán completamente predecibles.

10.14. Sistema de despacho

Cuando una alerta sea confirmada:

Evento-prioridad-unidad disponible-despacho-seguimiento-llegada-resultado-cierre

Esto permitirá conocer exactamente cuánto tiempo transcurrió desde la detección hasta la intervención.

10.15. Tiempo de respuesta

Cada evento permitirá calcular:

1. Tiempo de detección.
2. Tiempo de validación.
3. Tiempo de despacho.
4. Tiempo de llegada.
5. Tiempo de resolución.

Estos indicadores permitirán identificar problemas operacionales reales.

10.16. Comunicaciones seguras

Las unidades deberán disponer de canales de comunicación confiables y protegidos. En sectores críticos se buscará redundancia mediante:

a) Fibra;

b) Redes de radio;

c) Conectividad móvil;

d) Sistemas alternativos cuando corresponda.

10.17. Energía

Cada nodo crítico deberá disponer de respaldo. Podrán combinarse:

a) Red eléctrica;

b) Baterías;

c) Generadores;

d) Sistemas solares;

e) Otras soluciones apropiadas.

10.18. Autodiagnóstico

Los sensores deberán informar automáticamente:

a) Pérdida de conexión;

b) Cámara bloqueada;

c) Batería baja;

d) Sobrecalentamiento;

e) Fallo de almacenamiento;

f) Manipulación;

g) Interrupción eléctrica.

Un sensor fuera de servicio debe convertirse automáticamente en un incidente técnico.

10.19. Manipulación física

Los dispositivos deberán incorporar mecanismos para detectar intentos de:

a) Desconexión;

b) Movimiento no autorizado;

c) Obstrucción;

d) Daño;

e) Sabotaje.

10.20. Mantenimiento preventivo

Cada equipo tendrá un expediente digital que registre:

a) Instalación;

b) Garantía;

c) Mantenimientos;

d) Reparaciones;

e) Piezas sustituidas;

f) Tiempo fuera de servicio;

g) Vida útil.

Esto evitará que el Estado adquiera tecnología costosa que termine abandonada por falta de mantenimiento.

10.21. Inventario tecnológico en tiempo real

SIGFRO-RD permitirá visualizar:

- Equipos instalados
- Operativos
- Fuera de servicio
- En reparación
- Próximos a mantenimiento.

La disponibilidad tecnológica se convertirá en un indicador institucional.

10.22. Privacidad

Las cámaras fronterizas deberán orientarse primordialmente hacia objetivos de seguridad, control e infraestructura fronteriza.

Cuando existan poblaciones cercanas, deberán adoptarse medidas para evitar vigilancia innecesaria de actividades privadas ajenas a las finalidades del sistema.

10.23. Conservación de imágenes

No todas las imágenes deberán conservarse indefinidamente. La futura regulación deberá establecer distintos plazos considerando:

a) Videos ordinarios;

b) Eventos relevantes;

c) Evidencia administrativa;

d) Evidencia penal;

e) Incidentes de seguridad;

f) Investigaciones abiertas.

10.24. Acceso a grabaciones

El acceso quedará registrado. El sistema deberá indicar quién vio el video, cuándo, cuál video, motivo, si realizó exportación.

10.25. Exportación de evidencia

Cuando una grabación sea necesaria para investigación administrativa o penal deberá generarse una copia técnicamente verificable. Se deberá garantizar integridad, fecha, fuente, cadena de custodia, Hash o mecanismo equivalente, identidad del funcionario que realizó la extracción.

10.26. Protección ambiental

La misma infraestructura podrá contribuir, dentro de las competencias correspondientes, a detectar:

a) Incendios;

b) Tala;

c) Movimientos irregulares asociados a extracción de recursos;

d) Afectaciones de áreas protegidas;

e) Otros eventos ambientales.

Esto aumentará el rendimiento de la inversión tecnológica.

10.27. Seguridad de la información

Cámaras, sensores y radares serán considerados potenciales puntos de entrada para ataques cibernéticos. Por ello deberán cumplir:

a) Credenciales únicas;

b) Actualización de firmware;

c) Segmentación de redes;

d) Cifrado;

e) Monitoreo;

f) Control de proveedores;

g) Inventario de vulnerabilidades.

10.28. Prohibición de contraseñas de fábrica

Ningún equipo deberá permanecer operativo con usuarios o contraseñas predeterminadas por el fabricante. El cumplimiento deberá comprobarse antes de la aceptación técnica.

10.29. Indicadores operacionales

La red deberá medir:

a) Porcentaje de frontera con cobertura tecnológica;

b) Sensores disponibles;

c) Sensores fuera de servicio;

d) Alertas generadas;

e) Alertas confirmadas;

f) Falsas alarmas;

g) Tiempo medio de respuesta;

h) Incidentes detectados;

i) Disponibilidad de comunicaciones;

j) Disponibilidad energética.

10.30. Resultado esperado

La vigilancia electrónica deberá permitir evolucionar desde un modelo donde el Estado descubre el evento cuando un patrullero lo observa hacia otro donde el sistema detecta → verifica → geolocaliza → alerta → orienta la respuesta → registra el resultado.

CAPÍTULO XI

SISTEMA NACIONAL DE DRONES FRONTERIZOS

11.1. Concepto

Se propone estructurar un **Sistema Nacional de Drones Fronterizos —SINADROF—**, integrado operacionalmente a SIGFRO-RD y a las capacidades de comando, control, comunicaciones, ciberseguridad e inteligencia de las Fuerzas Armadas.

SINADROF no deberá entenderse exclusivamente como la adquisición de aeronaves no tripuladas. Constituirá un sistema compuesto por:

a) Aeronaves;

b) Estaciones de control;

c) Bases y estaciones automáticas;

d) Comunicaciones;

e) Sensores;

f) Software;

g) Pilotos y operadores;

h) Protocolos operativos;

i) Mantenimiento;

j) Analítica de imágenes;

k) Integración con centros de mando;

l) Seguridad cibernética;

m) Regulación y supervisión operacional.

11.2. Aprovechamiento de capacidades existentes

La República Dominicana ya dispone de capacidades relevantes sobre las cuales construir este sistema. En febrero de 2026 el Poder Ejecutivo informó sobre la incorporación de drones autónomos y tecnología anti-UAV, vinculándolos directamente con el fortalecimiento del Centro de Comando, Control, Comunicaciones, Ciberseguridad e Inteligencia —C5i— de las Fuerzas Armadas.

Consecuentemente, la política propuesta no deberá crear una flota paralela sin coordinación. Deberá inventariar, integrar, estandarizar, ampliar y mantener.

11.3. Objetivos operacionales

Los drones fronterizos podrán ser utilizados para:

a) Vigilancia de sectores de difícil acceso;

b) Verificación de alertas generadas por sensores;

c) Seguimiento visual de acontecimientos;

d) Patrullaje programado;

e) Reconocimiento nocturno;

f) Evaluación de rutas;

g) Inspección de infraestructura;

h) Supervisión de la verja;

i) Localización de daños;

j) Detección de incendios;

k) Vigilancia ambiental dentro de las competencias correspondientes;

l) Apoyo en operaciones de búsqueda y rescate;

m) Evaluación posterior a desastres;

n) Obtención legítima de evidencia audiovisual.

11.4. Principio de verificación aérea

Una de las funciones principales será verificar eventos antes de comprometer recursos terrestres.

Ejemplo:

Sensor detecta movimiento/Cámara térmica confirma actividad/Dron recibe coordenadas/Dron verifica naturaleza del evento/Centro de mando determina nivel de respuesta/Unidad terrestre es despachada cuando corresponda.

Esto permitirá utilizar racionalmente los recursos humanos.

11.5. Categorías de drones

La flota podrá organizarse funcionalmente en:

a) Drones de corto alcance	Destinados a unidades de patrullaje para reconocimiento inmediato.

b) Drones de vigilancia sectorial	Con mayor autonomía, utilizados para cubrir zonas previamente definidas.
c) Drones autónomos de estación	Instalados en bases automáticas capaces de despegar, ejecutar determinadas rutas, regresar y recargarse con mínima intervención humana, siempre dentro de las autorizaciones aplicables.
d) Sistemas especializados	Destinados a misiones técnicas específicas, tales como cartografía, inspección de infraestructura o vigilancia térmica.
11.6. Estaciones automáticas	En sectores estratégicos podrán instalarse estaciones capaces de: a) Alojar el dron; b) Recargar baterías; c) Proteger equipos; d) Ejecutar autodiagnósticos; e) Descargar información; f) Actualizar planes de vuelo; g) Transmitir video; h) Alertar sobre daños; i) Registrar aperturas de la estación.

11.7. Cobertura por cuadrantes

El espacio fronterizo podrá dividirse en cuadrantes operacionales. Cada cuadrante tendrá identificado:

a) Base más próxima;

b) Drones disponibles;

c) Autonomía;

d) Tiempo estimado de llegada;

e) Sensores terrestres existentes;

f) Unidades terrestres disponibles;

g) Condiciones de comunicación.

SIGFRO-RD podrá seleccionar automáticamente el recurso disponible más apropiado.

11.8. Patrullaje programado

Las aeronaves podrán ejecutar rutas preventivas. Estas rutas no deberán ser completamente predecibles. El sistema podrá variar:

a) Horario;

b) Altitud;

c) Secuencia;

d) Duración;

e) Área;

11.9. Patrullaje orientado por riesgo

La información histórica permitirá incrementar temporalmente la vigilancia en sectores que presenten patrones anormales. El principio será mayor riesgo comprobado / mayor vigilancia temporal. No vigilancia permanente e indiscriminada de toda actividad humana.

11.10. Regulación aeronáutica

La operación deberá armonizarse con la legislación aeronáutica dominicana y con las disposiciones del Instituto Dominicano de Aviación Civil —IDAC— en todo aquello que resulte aplicable a las operaciones correspondientes.

El IDAC mantiene actualmente el marco regulatorio de los sistemas de aeronaves no tripuladas mediante el **RAD 107**, además de requisitos de registro, licencias, autorizaciones especiales y seguridad operacional.

Las operaciones militares o de seguridad que dispongan de regímenes especiales deberán coordinarse conforme al ordenamiento jurídico correspondiente, evitando conflictos con la navegación aérea civil.

11.11. Geocercas digitales

Los sistemas deberán incorporar geofencing o mecanismos equivalentes para evitar:

a) Entrada accidental en espacio restringido;

b) Aproximación indebida a aeropuertos;

c) Interferencia con aeronaves tripuladas;

d) Salida del área operacional autorizada;

e) Cruces territoriales no autorizados.

11.12. Respeto de la línea internacional

Los planes de vuelo deberán incorporar mecanismos técnicos para evitar que una aeronave estatal dominicana cruce accidentalmente el límite internacional cuando la misión no disponga de fundamento jurídico para ello. La geocerca fronteriza deberá incorporar márgenes de seguridad.

11.13. Operación nocturna

Las aeronaves destinadas a vigilancia nocturna podrán incorporar:

a) Sensores térmicos;

b) Cámaras de baja luminosidad;

c) Sistemas infrarrojos;

d) Iluminación cuando resulte operacionalmente conveniente.

11.14. Transmisión en tiempo real

Cuando la conectividad lo permita, el video deberá transmitirse directamente al centro operacional correspondiente. El operador en terreno y el centro de mando podrán observar simultáneamente la misión cuando el nivel del evento así lo requiera.

11.15. Grabaciones

Las grabaciones deberán quedar vinculadas al Identificador Único de Evento Fronterizo correspondiente. Se registrará:

a) Dron;

b) Piloto u operador;

c) Fecha;

d) Hora;

e) Trayectoria;

f) Cámara utilizada;

g) Evento relacionado;

h) Archivo producido.

11.16. Integridad de evidencia

Cuando una grabación deba utilizarse como evidencia administrativa o penal, deberá conservarse su integridad mediante mecanismos técnicos verificables y cadena de custodia.

11.17. Inteligencia artificial a bordo

Determinados drones podrán incorporar sistemas capaces de detectar:

a) Personas;

b) Vehículos;

c) Embarcaciones;

d) Animales;

e) Incendios;

f) Objetos;

g) Cambios relevantes en infraestructura.

Estas capacidades tendrán carácter auxiliar.

11.18. Prohibición de decisión coercitiva autónoma

Dentro de la presente política ningún dron podrá decidir autónomamente detener, perseguir físicamente, atacar o emplear fuerza contra una persona. Los sistemas podrán detectar, identificar probabilísticamente, seguir e informar.

La actuación coercitiva corresponderá exclusivamente a las autoridades competentes bajo las reglas legales aplicables.

11.19. Drones armados

La presente política de tecnificación y gestión fronteriza no contempla drones armados ni sistemas autónomos de empleo de fuerza.

Cualquier política estatal futura sobre capacidades militares de naturaleza distinta deberá poseer fundamento jurídico, doctrinal y operacional propio y permanecer fuera del alcance de este Documento Marco.

11.20. Tecnología anti-UAV

El fortalecimiento de la frontera deberá considerar también la amenaza que representan drones no autorizados.

Podrán utilizarse tecnologías destinadas a:

a) Detectar;

b) Clasificar;

c) Localizar;

d) Seguir;

e) Identificar;

f) Neutralizar legalmente cuando corresponda, aeronaves no tripuladas que representen una amenaza.

El Gobierno dominicano ya informó en 2026 la incorporación de tecnología anti-UAV dentro del proceso de modernización de defensa.

11.21. Registro de drones autorizados

Toda aeronave integrada al sistema deberá disponer de un expediente digital que incluya:

a) Número institucional;

b) Serie;

c) Modelo;

d) Propietario estatal;

e) Base asignada;

f) Características técnicas;

g) Sensores;

h) Firmware;

i) Mantenimientos;

j) Reparaciones;

k) Baterías asignadas;

l) Historial de vuelo.

11.22. Control de firmware

Las actualizaciones deberán realizarse mediante procedimientos autorizados. Se evitará que un proveedor pueda modificar remotamente equipos críticos sin conocimiento del Estado dominicano.

11.23. Soberanía tecnológica

En las adquisiciones deberán evaluarse:

a) Ubicación de servidores;

b) Dependencia de servicios extranjeros;

c) Acceso del fabricante a información;

d) Capacidad de operación sin conexión externa;

e) Disponibilidad de repuestos;

f) Control de actualizaciones;

g) Propiedad de datos;

h) Capacidad nacional de mantenimiento.

11.24. Indicadores

SINADROF deberá medir:

a) Horas de vuelo;

b) Misiones ejecutadas;

c) Eventos verificados;

d) Tiempo promedio de respuesta aérea;

e) Disponibilidad de aeronaves;

f) Fallas;

g) Accidentes;

h) Incidentes;

i) Misiones abortadas;

j) Porcentaje de falsas alertas descartadas mediante verificación aérea;

k) Costos operacionales por hora;

l) Cobertura territorial.

CAPÍTULO XII

CENTRO NACIONAL DE COMANDO E INTELIGENCIA FRONTERIZA

12.1. Criterio institucional

La República Dominicana ya dispone del Centro de Comando, Control, Comunicaciones, Ciberseguridad e Inteligencia —C5i— dentro de sus capacidades de defensa.

Por tanto, crear otro gran centro nacional independiente podría duplicar infraestructura y responsabilidades.

La presente política propone que el Centro Nacional de Comando e Inteligencia Fronteriza —CNCIF— sea concebido como una capacidad especializada de gestión fronteriza articulada con el C5i, y no como una nueva entidad pública autónoma.

El fortalecimiento del C5i mediante drones autónomos, tecnología anti-UAV y nuevas capacidades fue expresamente reportado por el Poder Ejecutivo en 2026.

12.2. Modelo distribuido

El sistema deberá operar mediante centro nacional, centros regionales, puestos locales y unidades móviles. No toda decisión deberá desplazarse hacia Santo Domingo.

El propósito será combinar coordinación nacional con autonomía operacional territorial.

12.3. Centros regionales

Podrán establecerse o adaptarse capacidades regionales vinculadas a los principales sectores fronterizos. Estos centros deberán recibir información de:

a) Cámaras;

b) Sensores;

c) Drones;

d) Radares;

e) Unidades terrestres;

f) Puestos fronterizos;

g) Sistemas autorizados de otras instituciones.

12.4. Imagen operacional común

La plataforma deberá generar una Imagen Operacional Común de Frontera —IOCF—.

Esta imagen podrá representar, según el nivel de autorización del usuario:

a) Eventos abiertos;

b) Sensores disponibles;

c) Alertas;

d) Unidades operativas;

e) Vehículos oficiales;

f) Drones;

g) Zonas de riesgo;

h) Incidencias tecnológicas;

i) Condiciones meteorológicas;

j) Infraestructura crítica.

12.5. Compartimentación

La existencia de una imagen operacional común no significa que todos los usuarios observen todo.

El sistema tendrá distintos niveles de clasificación y acceso.

Un operador podrá conocer que existe una alerta sin acceder necesariamente al contenido de una investigación reservada.

12.6. Sala de operaciones

La sala correspondiente deberá disponer de puestos especializados para:

a) Vigilancia territorial;

b) Operaciones aéreas no tripuladas;

c) Comunicaciones;

d) Coordinación terrestre;

e) Incidentes tecnológicos;

f) Inteligencia;

g) Enlace interinstitucional;

h) Coordinación logística.

12.7. Oficiales de enlace

En operaciones de especial complejidad podrán participar oficiales o funcionarios de enlace de instituciones como:

a) Dirección General de Migración;

b) Dirección General de Aduanas;

c) Autoridades de seguridad;

d) Organismos de inteligencia competentes;

e) Salud Pública;

f) Agricultura;

g) Medio Ambiente;

h) Ministerio Público cuando jurídicamente corresponda.

La presencia de un enlace no transferirá competencias.

12.8. Ciclo del evento

Todo evento deberá recorrer una secuencia operacional:

Detección → recepción → validación → clasificación → asignación → respuesta → supervisión → resolución → cierre → evaluación.

12.9. Clasificación inicial

El sistema podrá clasificar los eventos en:

Nivel 1 — Informativo No requiere intervención inmediata.

Nivel 2 — Preventivo Requiere observación o verificación.

Nivel 3 — Operacional	Requiere actuación de una unidad.
Nivel 4 — Crítico	Puede implicar amenaza grave, delito, emergencia o riesgo para personas o infraestructura.

12.10. Escalamiento

Una alerta podrá aumentar o disminuir de nivel según la información obtenida. Cada cambio deberá registrar:

a) Hora;

b) Operador;

c) Motivo;

d) Información considerada.

12.11. Despacho asistido

La plataforma podrá recomendar la unidad más apropiada considerando:

a) Ubicación;

b) Especialidad;

c) Disponibilidad;

d) Tiempo de llegada;

e) Tipo de evento;

f) Recursos necesarios.

La decisión final corresponderá al responsable operacional.

12.12. Seguimiento de unidades

Durante eventos operacionales, el centro podrá conocer la ubicación de las unidades oficiales asignadas cuando la tecnología disponible lo permita. Esto aumentará:

a) Seguridad del personal;

b) Coordinación;

c) Tiempo de respuesta;

d) Capacidad de apoyo.

12.13. Botón de emergencia

Las unidades podrán disponer de un mecanismo de emergencia capaz de enviar:

a) Identidad;

b) Posición;

c) Unidad;

d) Hora;

e) Evento relacionado.

12.14. Grabación de decisiones críticas

Determinadas decisiones operacionales de importancia deberán quedar documentadas electrónicamente. No será suficiente registrar únicamente el resultado.

El sistema deberá permitir determinar posteriormente cómo se desarrolló el acontecimiento.

12.15. Bitácora digital de turno

Cada centro mantendrá una bitácora electrónica. Deberá registrar:

a) Inicio del turno;

b) Personal;

c) Equipos fuera de servicio;

d) Alertas abiertas;

e) Eventos relevantes;

f) Traspaso de novedades;

g) Finalización del turno.

12.16. Relevo formal

El cambio de turno deberá realizarse electrónicamente. El nuevo supervisor deberá confirmar la recepción de:

a) Eventos pendientes;

b) Fallas;

c) Operaciones abiertas;

d) Información crítica.

12.17. Inteligencia fronteriza

La inteligencia producida no deberá limitarse a incidentes individuales. El centro podrá identificar:

a) Patrones horarios;

b) Sectores recurrentes;

c) Modificaciones de rutas;

d) Relaciones entre eventos;

e) Nuevas modalidades operativas;

f) Evolución del riesgo.

12.18. Separación entre inteligencia y prueba

Un resultado de inteligencia puede justificar vigilancia o investigación adicional. No deberá confundirse automáticamente con evidencia suficiente para sancionar. La eventual utilización judicial deberá cumplir los requisitos legales correspondientes.

12.19. Protección frente al uso político

Los sistemas fronterizos no deberán utilizarse para vigilancia de:

a) Adversarios políticos;

b) Periodistas;

c) Activistas;

d) Ciudadanos;

e) Funcionarios, por razones ajenas a las competencias y finalidades legalmente atribuidas al sistema. Toda consulta deberá ser auditable.

12.20. Evaluación posterior del evento

Los acontecimientos de importancia deberán generar un proceso de revisión. Se evaluará:

a) Qué ocurrió;

b) Cómo fue detectado;

c) Tiempo de respuesta;

d) Recursos utilizados;

e) Resultado;

f) Fallas;

g) Lecciones aprendidas;

h) Correcciones necesarias.

12.21. Simulacros

El sistema deberá realizar periódicamente ejercicios que incluyan:

a) Cruce irregular masivo;

b) Contrabando;

c) Ataque a infraestructura;

d) Fallo de comunicaciones;

e) Ciberataque;

f) Incendio;

g) Evento sanitario;

h) Desastre natural;

i) Incursión de dron no autorizado.

12.22. Indicadores

Entre los principales indicadores:

a) Tiempo de detección;

b) Tiempo de validación;

c) Tiempo de despacho;

d) Tiempo de llegada;

e) Tiempo de resolución;

f) Eventos resueltos;

g) Falsas alarmas;

h) Eventos escalados;

i) Disponibilidad del centro;

j) Incidencias por turno.

CAPÍTULO XIII

INTEROPERABILIDAD DE LAS BASES DE DATOS ESTATALES

13.1. Principio fundamental

La verdadera tecnificación fronteriza no depende de tener una sola gran base de datos. Depende de lograr que las bases existentes puedan comunicarse de forma segura, controlada y jurídicamente válida.

República Dominicana dispone actualmente de la NORTIC A4:2024, cuya versión oficial fue actualizada el 23 de junio de 2026 y que establece estándares para la interoperabilidad y el intercambio seguro de información mediante la Plataforma Única de Interoperabilidad.

13.2. Modelo federado

SIGFRO-RD utilizará prioritariamente un modelo federado.

Esto significa:

> *Institución A conserva sus datos / SIGFRO-RD realiza consulta autorizada / Institución A responde únicamente lo permitido / SIGFRO-RD registra la consulta y continúa el proceso.*

13.3. Prohibición de copia masiva innecesaria

No deberán copiarse bases completas hacia SIGFRO-RD cuando una consulta en tiempo real permita cumplir la misma finalidad. La centralización excesiva aumentaría el riesgo cibernético, el impacto de una filtración, duplicidad, inconsistencias, así como responsabilidad administrativa.

13.4. Principios NORTIC

La arquitectura deberá considerar las cuatro dimensiones de interoperabilidad que recoge NORTIC A4:

a) Organizacional;

b) Semántica;

c) Jurídica;

d) Técnica.

Esto es particularmente importante porque conectar técnicamente dos sistemas no significa que jurídicamente puedan intercambiar cualquier información.

13.5. Catálogo de datos fronterizos

Se elaborará un catálogo que identifique:

a) Dato;

b) Institución responsable;

c) Definición;

d) Formato;

e) Nivel de sensibilidad;

f) Base jurídica;

g) Usuarios autorizados;

h) Finalidad;

i) Período de conservación cuando corresponda;

j) Frecuencia de actualización.

13.6. Institución fuente

Cada dato deberá tener una fuente oficial primaria. Ejemplo conceptual:

Información migratoria → Migración

Información aduanera → Aduanas

La plataforma no deberá alterar unilateralmente información perteneciente a otra institución.

13.7. Calidad de datos

La institución fuente será responsable de establecer mecanismos para:

a) Validación;

b) Actualización;

c) Corrección;

d) Resolución de duplicidades;

e) Control de integridad.

SIGFRO-RD deberá poder reportar inconsistencias a la institución responsable.

13.8. Respuestas mínimas

Cuando sea posible, las consultas deberán utilizar respuestas limitadas.

Ejemplo:

En lugar de entregar todo un expediente:

Documento válido: Sí/No.

Alerta vigente: Sí/No.

Vehículo registrado: Sí/No.

Autorización válida: Sí/No.

Esto reduce exposición innecesaria de información.

13.9. Interfaces de programación

Los intercambios deberán realizarse mediante APIs u otros mecanismos seguros definidos por los estándares estatales. Cada interfaz deberá disponer de:

a) Autenticación;

b) Autorización;

c) Cifrado;

d) Límites de consulta;

e) Registro;

f) Versionado;

g) Monitoreo.

13.10. Registro de consultas

Toda consulta relevante deberá registrar:

institución solicitante → usuario → dato solicitado → finalidad → fecha → resultado.

Este registro deberá protegerse contra modificaciones no autorizadas.

13.11. Acceso por finalidad

Tener capacidad técnica para acceder a un dato no equivale a tener autorización jurídica.

Cada consulta deberá estar asociada a una finalidad institucional válida.

13.12. Datos biométricos

Los datos biométricos deberán permanecer bajo controles particularmente estrictos.

Cuando sea suficiente recibir el resultado de una comparación, no será necesario entregar la plantilla biométrica original.

Ejemplo:

Coincidencia validada : Sí.

en lugar de : Entregar archivo completo de huellas.

13.13. Datos de inteligencia

La interoperabilidad con sistemas de inteligencia deberá utilizar mecanismos de compartimentación. Podrá transmitirse: "Existe alerta — contactar unidad competente" sin revelar necesariamente:

a) Fuente;

b) Investigación;

c) Técnica utilizada;

d) Información clasificada.

13.14. Identificadores comunes

Cuando sea jurídicamente posible podrán utilizarse identificadores normalizados para relacionar:

a) Personas;

b) Vehículos;

c) Empresas;

d) Operadores;

e) Declaraciones;

f) Eventos.

El sistema deberá evitar identificar personas únicamente mediante nombres, debido a errores, homónimos y variaciones ortográficas.

13.15. Resolución de identidades

SIGFRO-RD podrá utilizar mecanismos que detecten posibles registros correspondientes a una misma persona o entidad. El resultado tendrá carácter de posible correspondencia. La consolidación definitiva corresponderá a la institución responsable.

13.16. Interoperabilidad semántica

Todas las instituciones deberán comprender los datos de la misma manera. Por ejemplo, conceptos como entrada, salida, vehículo activo, alerta vigente, inspección completada, evento cerrado deberán poseer definiciones comunes dentro del catálogo.

13.17. Sello de tiempo

Los eventos deberán utilizar referencias temporales sincronizadas. Esto permitirá reconstruir secuencias con precisión.

13.18. Operación asincrónica

Cuando un sistema institucional se encuentre temporalmente fuera de servicio, SIGFRO-RD podrá:

a) Mantener solicitud pendiente;

b) Reintentar;

c) Aplicar procedimientos de contingencia;

d) Notificar al operador;

e) Registrar la indisponibilidad.

Nunca deberá convertir automáticamente una ausencia de respuesta en una respuesta positiva.

13.19. Principio de fallo seguro

Cuando una consulta crítica no pueda completarse **"no se pudo verificar"** no deberá convertirse automáticamente en **"verificado".** El procedimiento de contingencia dependerá del tipo de operación.

13.20. Monitoreo de interoperabilidad

La plataforma medirá:

a) Consultas realizadas;

b) Tiempo de respuesta;

c) Errores;

d) Sistemas indisponibles;

e) Consultas rechazadas;

f) Volumen de intercambio;

g) Incidentes de seguridad.

13.21. Convenios e instrumentos jurídicos

Cuando las normas existentes no resulten suficientes, las instituciones deberán establecer los instrumentos jurídicos correspondientes para definir:

a) Datos intercambiables;

b) Finalidades;

c) Responsabilidades;

d) Seguridad;

e) Conservación;

f) Auditoría;

g) Procedimientos ante incidentes.

13.22. Derecho de corrección

Cuando una persona pueda ejercer legalmente derechos de acceso, rectificación o corrección sobre datos personales, la corrección deberá realizarse ante la institución responsable del registro original.

SIGFRO-RD deberá posteriormente consumir el dato corregido.

13.23. Resultado esperado

La interoperabilidad deberá permitir que el funcionario competente obtenga la información necesaria, de la fuente correcta, en el momento necesario y únicamente para la finalidad autorizada.

CAPÍTULO XIV

INTELIGENCIA ARTIFICIAL Y ANÁLISIS PREDICTIVO

14.1. Marco nacional

La República Dominicana posee desde 2023 una Estrategia Nacional de Inteligencia Artificial —ENIA—, formalizada mediante el Decreto núm. 498-23. OGTIC define la ENIA como la estrategia nacional orientada al desarrollo y utilización eficiente y segura de la inteligencia artificial. La política de Frontera Inteligente deberá alinearse con esa estrategia y no desarrollar un modelo de inteligencia artificial completamente separado del marco nacional.

14.2. Objetivo

La inteligencia artificial se utilizará para aumentar la capacidad humana de:

a) Observar;

b) Clasificar;

c) Comparar;

d) Detectar anomalías;

e) Priorizar;

f) Predecir necesidades operativas;

g) Mantener infraestructura.

No deberá utilizarse como sustituto automático de la autoridad.

14.3. Principio rector

La regla fundamental será "La IA recomienda; la autoridad competente decide."

14.4. Usos permitidos

La IA podrá utilizarse, entre otros, para:

a) Analítica de video;

b) Detección de objetos;

c) Reconocimiento de matrículas;

d) Identificación de anomalías vehiculares;

e) Correlación de eventos;

f) Análisis de rutas;

g) Gestión de colas;

h) Predicción de congestionamientos;

i) Mantenimiento predictivo;

j) Distribución de recursos;

k) Detección de patrones de fraude;

l) Priorización de alertas;

m) Apoyo al análisis aduanero dentro de las competencias correspondientes.

14.5. Analítica de video

Los sistemas podrán analizar transmisiones para identificar potencialmente:

a) Personas;

b) Grupos;

c) Vehículos;

d) Motocicletas;

e) Animales;

f) Objetos abandonados;

g) Movimiento en zonas restringidas.

La clasificación deberá expresarse probabilísticamente y someterse a verificación cuando vaya a generar una actuación relevante.

14.6. Correlación temporal

La IA podrá identificar relaciones que resultarían difíciles de detectar manualmente.

Ejemplo:

- Vehículo X aparece en tres eventos.
- Conductor Y aparece repetidamente con X.
- Carga Z presenta inconsistencias similares.
- Los eventos ocurren bajo un mismo patrón horario.

El sistema podrá generar **"**Patrón relevante — requiere análisis". No: "Delito comprobado".

14.7. Análisis predictivo

Los modelos podrán estimar:

a) Sectores con mayor probabilidad de determinados eventos;

b) Horarios de mayor actividad;

c) Necesidad de personal;

d) Congestión de puntos fronterizos;

e) Probabilidad de falla de equipos;

f) Demanda logística.

14.8. Patrullaje predictivo

Los algoritmos podrán recomendar distribución de patrullaje. Sin embargo, deberá evitarse una retroalimentación defectuosa donde más patrullas, más detecciones, sistema concluye que existe más riesgo, envía todavía más patrullas.

Los modelos deberán distinguir entre actividad real y actividad observada debido a mayor vigilancia.

14.9. Perfil de riesgo

Un sistema automatizado podrá producir perfiles de riesgo sobre operaciones o eventos. Las variables deberán:

a) Tener relación objetiva con la finalidad;

b) Ser legalmente utilizables;

c) Documentarse;

d) Evaluarse periódicamente;

e) Someterse a auditoría.

14.10. Prohibición de perfilamiento étnico

No deberá utilizarse inteligencia artificial para inferir o atribuir irregularidad a una persona sobre la base de:

a) Color de piel;

b) Rasgos físicos;

c) Etnicidad real o percibida;

d) Otros atributos personales constitucionalmente protegidos.

El control migratorio deberá basarse en estatus, documentación, autorización y hechos legalmente relevantes, no en apariencia física.

14.11. Nacionalidad y situación migratoria

Cuando la nacionalidad o estatus migratorio sea jurídicamente relevante para un procedimiento, deberá determinarse mediante documentos, registros y mecanismos legalmente establecidos.

No mediante inferencias algorítmicas basadas en apariencia, idioma o acento.

14.12. Decisiones de alto impacto

Se considerarán decisiones de alto impacto aquellas que puedan conducir a:

a) Detención;

b) Rechazo migratorio;

c) Deportación;

d) Incautación;

e) Sanción;

f) Investigación penal;

g) Restricción significativa de derechos.

En estos casos la decisión final deberá ser humana y jurídicamente motivada.

14.13. Registro Nacional de Modelos Fronterizos

Se propone mantener un inventario técnico de los modelos de IA utilizados.

Cada modelo deberá registrar:

a) Nombre;

b) Función;

c) Institución responsable;

d) Proveedor;

e) Versión;

f) Datos utilizados para entrenamiento cuando sean conocidos;

g) Variables principales;

h) Fecha de implementación;

i) Nivel de riesgo;

j) Resultados de evaluación;

k) Fecha de última revisión.

14.14. Versionado

Cuando un modelo sea actualizado deberá conservarse información sobre la versión anterior. Esto permitirá determinar posteriormente qué versión produjo una alerta específica.

14.15. Pruebas previas

Antes de pasar a producción, todo modelo de alto impacto deberá evaluarse utilizando datos representativos. Se analizará:

a) Precisión;

b) Falsos positivos;

c) Falsos negativos;

d) Robustez;

e) Sesgos;

f) Vulnerabilidades;

g) Rendimiento bajo condiciones adversas.

14.16. Evaluación periódica

Un modelo que funcionó correctamente al inicio puede perder precisión con el tiempo. Por ello deberán realizarse pruebas periódicas.

14.17. Umbrales configurables

Los niveles de confianza requeridos deberán variar según el uso.

Ejemplo:

Una probabilidad moderada puede ser suficiente para que una cámara amplíe una imagen. No necesariamente para ordenar una inspección intrusiva.

14.18. Explicabilidad

Cuando una alerta automatizada produzca una intervención significativa, el funcionario deberá recibir, cuando técnicamente sea posible, información sobre los factores principales que generaron la alerta. No deberá limitarse a **"l**a computadora dijo riesgo alto".

14.19. Supervisión humana

Los operadores deberán poder:

a) Confirmar;

b) Rechazar;

c) Escalar;

d) Solicitar nueva verificación.

Pero cada intervención humana deberá quedar registrada.

14.20. Anulación de alerta

Cuando un funcionario descarte una alerta deberá seleccionar o explicar la causa.

Por ejemplo:

a) Falsa lectura;

b) Identidad confirmada;

c) Operación legítima;

d) Fallo del sensor;

e) Error documental posteriormente corregido.

Esto permitirá mejorar los algoritmos.

14.21. IA generativa

Las herramientas generativas podrán utilizarse para:

a) Resumir eventos;

b) Preparar borradores internos;

c) Consultar manuales;

d) Analizar grandes volúmenes de documentación no clasificada conforme a protocolos.

No deberán utilizarse para inventar datos faltantes. Toda información crítica deberá remontarse a su fuente original.

14.22. Datos clasificados y sistemas externos

Quedará prohibido introducir información clasificada o sensible en servicios públicos de IA externos no autorizados.

14.23. Desarrollo nacional

La ENIA contempla una estrategia nacional que incluye gobernanza, infraestructura, datos, talento e investigación. En ese contexto, el proyecto fronterizo podrá convertirse en un espacio para desarrollar capacidades dominicanas en:

a) Visión computacional;

b) Ciberseguridad;

c) Ingeniería de datos;

d) Robótica;

e) Sistemas autónomos;

f) Analítica geoespacial;

g) Mantenimiento tecnológico.

14.24. Indicadores

Se medirán:

a) Precisión;

b) Falsos positivos;

c) Falsos negativos;

d) Alertas confirmadas;

e) Tiempo ahorrado;

f) Modelos suspendidos;

g) Incidentes;

h) Sesgos detectados;

i) Versiones desplegadas;

j) Intervenciones humanas.

CAPÍTULO XV

CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

15.1. Principio esencial

Cuanto más tecnificada sea la frontera, mayor será su dependencia de sistemas digitales.

Una frontera inteligente sin ciberseguridad puede convertirse en una frontera vulnerable. Por tanto la ciberseguridad no será un componente adicional de SIGFRO-RD, será una condición de funcionamiento de SIGFRO-RD.

15.2. Marco nacional de ciberseguridad

República Dominicana dispone de la **Estrategia Nacional de Ciberseguridad 2030**, aprobada mediante el Decreto núm. 313-22, orientada a construir entornos digitales seguros, confiables y resilientes. El instrumento incluye expresamente la protección de infraestructuras críticas, gestión de riesgos, planes de continuidad y protocolos de respuesta a incidentes.

SIGFRO-RD deberá alinearse con este marco y con las directrices del Centro Nacional de Ciberseguridad —CNCS—.

15.3. Infraestructura crítica

Debido a su vinculación con:

a) Soberanía;

b) Defensa;

c) Migración;

d) Aduanas;

e) Seguridad;

f) Comercio;

g) Identidad;

h) Comunicaciones, deberá evaluarse formalmente la clasificación de los componentes esenciales de SIGFRO-RD como infraestructura crítica de información conforme al marco nacional aplicable.

15.4. Seguridad por diseño

Todo sistema deberá diseñarse partiendo de que será objeto potencial de:

a) Intrusión;

b) Sabotaje;

c) Robo de credenciales;

d) Manipulación de datos;

e) Ransomware;

f) Ataques de denegación;

g) Espionaje;

h) Ataques internos;

i) Compromiso de proveedores.

15.5. Modelo de confianza cero

Se adoptará progresivamente una arquitectura basada en "Nunca confiar automáticamente; verificar continuamente." Cada solicitud deberá considerar:

a) Usuario;

b) Dispositivo;

c) Ubicación;

d) Nivel de acceso;

e) Contexto;

f) Sensibilidad de la información.

15.6. Segmentación de redes

Los sistemas deberán separarse funcionalmente. Por ejemplo:

a) Red administrativa;

b) Red de cámaras;

c) Red de sensores;

d) Sistemas biométricos;

e) Sistemas críticos;

f) Red de invitados;

g) Mantenimiento.

Comprometer una cámara no deberá permitir automáticamente llegar a la base migratoria.

15.7. Separación IT/OT

Los sistemas tradicionales de información —IT— deberán segmentarse de los dispositivos operacionales —OT/IoT— como:

a) Barreras;

b) Cámaras;

c) Radares;

d) Sensores;

e) Lectores RFID;

f) Sistemas energéticos;

g) Estaciones de drones.

15.8. Identidad digital del funcionario

Todo usuario tendrá identidad individual. Quedarán prohibidas:

a) Cuentas compartidas;

b) Contraseñas genéricas;

c) Usuarios permanentes de proveedor;

d) Cuentas sin responsable.

15.9. Autenticación multifactor

Los sistemas críticos deberán utilizar MFA.

El propio CNCS recomienda mecanismos como autenticación de dos factores o multifactor para servicios sensibles y sistemas críticos.

15.10. Gestión de privilegios

Las cuentas administrativas requerirán controles superiores. Podrá implementarse gestión de acceso privilegiado —PAM— para registrar:

a) Inicio de sesión;

b) Duración;

c) Sistema;

d) Acciones;

e) Cambios;

f) Sesiones administrativas.

15.11. Proveedores

Los proveedores tecnológicos no deberán disponer de acceso permanente e ilimitado.

Los accesos remotos deberán:

a) Autorizarse;

b) Tener vigencia temporal;

c) Utilizar MFA;

d) Quedar registrados;

e) Supervisarse.

15.12. Cifrado

La información sensible deberá protegerse en tránsito y en reposo. Las llaves criptográficas deberán administrarse mediante procedimientos seguros.

15.13. Copias de seguridad

Las copias deberán:

a) Ejecutarse regularmente;

b) Cifrarse;

c) Mantener versiones;

d) Incluir copias aisladas cuando corresponda;

e) Someterse a pruebas reales de restauración.

Tener backup que nunca se ha intentado restaurar no constituye una garantía adecuada.

15.14. Centro de Operaciones de Seguridad

La infraestructura deberá permanecer bajo monitoreo continuo mediante capacidades SOC existentes o especializadas. Se deberá detectar:

a) Intentos de acceso;

b) Malware;

c) Comportamientos anómalos;

d) Exfiltración;

e) Cambios de configuración;

f) Actividad administrativa inusual;

g) Equipos comprometidos.

15.15. Integración con CSIRT-RD

Los incidentes deberán gestionarse coordinadamente con el Equipo Nacional de Respuesta a Incidentes Cibernéticos —CSIRT-RD— cuando corresponda.

La Estrategia Nacional de Ciberseguridad contempla expresamente protocolos de intercambio de información entre instituciones, infraestructuras críticas, equipos sectoriales y CSIRT-RD.

15.16. Plan de respuesta

SIGFRO-RD deberá disponer de procedimientos para:

a) Detección;

b) Contención;

c) Erradicación;

d) Recuperación;

e) Investigación;

f) Comunicación;

g) Lecciones aprendidas.

15.17. Escenarios prioritarios

Se deberán desarrollar planes específicos para:

a) Ransomware;

b) Robo de credenciales;

c) Manipulación de biometría;

d) Alteración de información vehicular;

e) Desactivación de cámaras;

f) Secuestro de drones;

g) GPS spoofing;

h) Interferencia de comunicaciones;

i) Ataque a infraestructura energética;

j) Exfiltración de datos.

15.18. Continuidad operacional

Un ciberataque no deberá necesariamente paralizar toda la frontera. Deberán definirse niveles de operación:

a) Operación normal.

b) Operación restringida.

c) Operación degradada.

d) Operación manual de emergencia.

e) Recuperación.

15.19. Pruebas de recuperación

Las instituciones deberán realizar simulaciones en las que se asuma que determinados sistemas han sido completamente comprometidos.

15.20. Actualizaciones

Los equipos deberán mantener firmware y software actualizado. Pero en sistemas críticos las actualizaciones deberán primero evaluarse para evitar que una actualización defectuosa provoque una interrupción masiva.

15.21. Inventario de activos

No se puede proteger lo que el Estado desconoce que posee. Cada activo deberá registrar:

a) Tipo;

b) Ubicación;

c) Responsable;

d) Dirección de red;

e) Fabricante;

f) Versión;

g) Criticidad;

h) Fecha de soporte;

i) Vulnerabilidades;

j) Estado.

15.22. Fin de soporte

Los equipos cuyo fabricante haya concluido actualizaciones de seguridad deberán ser identificados. SIGFRO-RD deberá mantener un programa de sustitución tecnológica.

15.23. Pruebas de penetración

Los componentes críticos deberán ser sometidos periódicamente a pruebas controladas realizadas por equipos autorizados.

Los hallazgos deberán clasificarse según nivel de riesgo y tener plazo de corrección.

15.24. Cadena de suministro

Antes de adquirir tecnologías críticas deberá evaluarse:

a) Fabricante;

b) País de origen cuando resulte relevante para el riesgo;

c) Actualizaciones;

d) Componentes;

e) Software incorporado;

f) Acceso remoto;

g) Subcontratistas;

h) Historial de vulnerabilidades;

i) Ubicación de servicios en la nube.

15.25. Protección de datos personales

El tratamiento de datos deberá armonizarse con el artículo 44 constitucional y con la Ley núm. 172-13 sobre protección integral de datos personales.

La Ley 172-13 establece principios y obligaciones vinculados con el tratamiento, calidad, seguridad y protección de información personal.

15.26. Clasificación de datos

Los datos podrán clasificarse, conforme al marco que se adopte, en categorías tales como:

a) Público;

b) Interno;

c) Confidencial;

d) Sensible;

e) Restringido o clasificado cuando jurídicamente corresponda.

15.27. Minimización

SIGFRO-RD recopilará los datos necesarios para una finalidad legítima. No todos los datos técnicamente posibles.

15.28. Períodos de conservación

Deberá existir una política diferenciada. No será razonable aplicar idéntico período a:

a) Video ordinario;

b) Evento de seguridad;

c) Registro migratorio;

d) Expediente aduanero;

e) Evidencia penal;

f) Log tecnológico.

Los plazos deberán derivarse de legislación, finalidad, necesidad y proporcionalidad.

15.29. Eliminación segura

Cuando corresponda destruir información, deberá utilizarse un proceso técnicamente verificable.

15.30. Registro de exportación

Cuando un usuario descargue información sensible deberá quedar registrado:

a) Usuario;

b) Archivo;

c) Fecha;

d) Motivo;

e) Destino cuando técnicamente sea posible.

15.31. Dispositivos extraíbles

El uso de memorias USB y otros medios extraíbles en sistemas críticos deberá limitarse estrictamente.

15.32. Prevención de fuga de información

Podrán utilizarse mecanismos para detectar y prevenir:

a) Envíos no autorizados;

b) Grandes extracciones;

c) Copias masivas;

d) Transferencias hacia servicios no autorizados.

15.33. Amenaza interna

El sistema deberá asumir que un ataque puede provenir también de un usuario autorizado. Podrán detectarse patrones como:

a) Consultas masivas;

b) Acceso fuera de horario;

c) Búsqueda de personas sin relación con funciones;

d) Exportaciones frecuentes;

e) Intentos de acceder a sistemas no autorizados.

15.34. Protección del funcionario

El monitoreo de usuarios deberá tener una finalidad institucional legítima y conocida.

No deberá convertirse en vigilancia arbitraria sobre la vida privada de los servidores públicos.

15.35. Formación

Todo funcionario deberá recibir capacitación proporcional a su función.

Se desarrollarán módulos sobre:

a) Phishing;

b) Contraseñas;

c) Ingeniería social;

d) Uso de dispositivos;

e) Datos personales;

f) Manejo de incidentes;

g) Información clasificada.

15.36. Certificación de personal crítico

Los puestos tecnológicos de mayor sensibilidad deberán requerir competencias verificables en materias como:

a) Redes;

b) Ciberseguridad;

c) Sistemas;

d) Bases de datos;

e) Forense digital;

f) Operaciones de infraestructura crítica.

15.37. Simulación de ciberataques

La Estrategia Nacional de Ciberseguridad 2030 contempla ejercicios de simulación para infraestructuras críticas e instituciones estatales. SIGFRO-RD deberá incorporarse periódicamente a este tipo de ejercicios.

15.38. Indicadores

Se medirán:

a) Incidentes;

b) Vulnerabilidades;

c) Tiempo de detección;

d) Tiempo de contención;

e) Tiempo de recuperación;

f) Sistemas parchados;

g) Cuentas privilegiadas;

h) Intentos de acceso;

i) Disponibilidad;

j) Copias restauradas exitosamente;

k) Funcionarios capacitados;

l) Incidentes de datos personales.

15.39. Principio final de seguridad

La seguridad tecnológica deberá diseñarse considerando que:

- Los equipos fallarán;
- Las comunicaciones podrán interrumpirse;
- Los usuarios cometerán errores;
- Existirán intentos de intrusión.

La resiliencia dependerá de que el sistema pueda prevenir, detectar, contener, continuar, recuperar y aprender.

CAPÍTULO XVI

INTEGRIDAD INSTITUCIONAL Y PREVENCIÓN DE LA CORRUPCIÓN FRONTERIZA

16.1. Principio general

La tecnificación de la frontera no alcanzará sus objetivos si los sistemas tecnológicos pueden ser manipulados, ignorados o utilizados discrecionalmente por quienes intervienen en los procesos.

Por tanto, uno de los propósitos centrales de SIGFRO-RD será reducir aquellas oportunidades de corrupción que puedan originarse mediante:

a) Autorizaciones discrecionales;

b) Registros manuales;

c) Pagos informales;

d) Alteración de documentos;

e) Eliminación de alertas;

f) Manipulación de inspecciones;

g) Selección interesada de funcionarios;

h) Omisión deliberada de controles;

i) Acceso indebido a información;

j) Coordinación irregular entre funcionarios y operadores privados.

El sistema deberá partir de una regla fundamental "Toda decisión relevante debe dejar evidencia digital verificable."

16.2. Marco jurídico

Las políticas de integridad asociadas a SIGFRO-RD deberán armonizarse, entre otras disposiciones, con:

a) La Constitución de la República;

b) La Ley núm. 41-08 de Función Pública;

c) La Ley núm. 10-07 que instituye el Sistema Nacional de Control Interno y de la Contraloría General de la República;

d) La Ley núm. 107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo;

e) La legislación penal aplicable;

f) La normativa sobre lavado de activos cuando corresponda;

g) Las normas de control interno emitidas por la Contraloría General de la República;

h) Los respectivos regímenes disciplinarios de las instituciones involucradas.

La Ley núm. 10-07 atribuye a las propias entidades públicas y a sus servidores responsabilidades directas en el establecimiento y mantenimiento de controles internos efectivos.

16.3. Contrataciones tecnológicas

La adquisición de equipos, plataformas, mantenimiento, licencias, infraestructura, servicios tecnológicos y demás componentes del proyecto deberá cumplir la legislación de contrataciones públicas vigente.

Desde el 28 de enero de 2026 se encuentra en vigor la Ley núm. 47-25 de Contrataciones Públicas, que sustituyó el régimen anterior como marco principal de contratación estatal. Por ello, las contrataciones de SIGFRO-RD deberán incorporar criterios específicos de:

a) Transparencia;

b) Competencia;

c) Seguridad nacional cuando corresponda;

d) Interoperabilidad;

e) Ciberseguridad;

f) Costo total de propiedad;

g) Mantenimiento;

h) Actualizaciones;

i) Transferencia tecnológica;

j) Disponibilidad de repuestos;

k) Protección de datos;

l) Soberanía tecnológica.

16.4. Prohibición de usuarios compartidos

Todo funcionario deberá operar mediante identidad individual. La plataforma deberá identificar exactamente a la persona que realizó cada actuación.

16.5. Firma o validación de actuaciones sensibles

Las operaciones de mayor impacto podrán requerir mecanismos reforzados de autenticación.

Ejemplos:

a) Anulación de una alerta;

b) Liberación extraordinaria de mercancía;

c) Modificación de registros sensibles;

d) Autorización excepcional;

e) Exportación masiva de información;

f) Desbloqueo de un vehículo con alerta;

g) Modificación posterior al cierre de un expediente.

16.6. Principio de doble control

Determinadas actuaciones podrán requerir autorización de dos funcionarios distintos. El modelo será:

Funcionario A solicita → Funcionario B valida.

Este procedimiento podrá aplicarse especialmente a:

a) Anulación de alertas críticas;

b) Correcciones posteriores;

c) Desbloqueo de controles;

d) Excepciones extraordinarias;

e) Exportaciones sensibles;

f) Operaciones administrativas de alta criticidad.

16.7. Segregación de funciones

El mismo funcionario no deberá controlar toda la cadena de una operación cuando sea técnicamente posible separarla.

Ejemplo:

Funcionario A recibe / Funcionario B inspecciona / Funcionario C autoriza / Sistema registra.

No todas las operaciones requerirán tres personas; la segregación deberá aplicarse según riesgo y complejidad.

16.8. Asignación automatizada de inspecciones

En aquellos procedimientos donde resulte jurídicamente y operacionalmente apropiado, los expedientes podrán distribuirse electrónicamente entre los inspectores disponibles. La plataforma podrá considerar:

a) Especialización;

b) Carga de trabajo;

c) Turno;

d) Disponibilidad;

e) Conflictos registrados;

f) Aleatoriedad controlada.

Esto dificultará acuerdos anticipados entre operadores y funcionarios específicos.

16.9. Reasignación

Un supervisor podrá modificar una asignación cuando exista causa justificada. Pero la plataforma registrará:

asignación original → reasignación → supervisor → motivo → fecha.

16.10. Rotación basada en riesgo

Las instituciones podrán establecer sistemas de rotación razonable en posiciones especialmente vulnerables. La rotación deberá:

a) Respetar la legislación de función pública y los regímenes especiales;

b) Evitar convertirse en instrumento arbitrario;

c) Preservar el conocimiento técnico;

d) Considerar áreas de elevada exposición a riesgos de corrupción.

16.11. Declaración de conflictos

Los funcionarios que intervengan en determinadas operaciones deberán disponer de mecanismos para informar potenciales conflictos de interés conforme al marco jurídico aplicable. Por ejemplo, cuando exista una relación personal o económica relevante con:

a) Empresas;

b) Transportistas;

c) Importadores;

d) Exportadores;

e) Operadores logísticos.

Cuando exista conflicto jurídicamente relevante, el expediente podrá ser reasignado.

16.12. Pagos electrónicos

La política procurará eliminar progresivamente el manejo de efectivo dentro de los procesos fronterizos estatales cuando existan mecanismos legalmente establecidos para realizar los pagos electrónicamente. La lógica será:

"Pago debido al Estado → pago registrado por canales oficiales."

16.13. Recibo digital

Todo pago deberá producir constancia verificable. El funcionario deberá poder confirmar pago válido: sí/no sin necesidad de manipular efectivo.

16.14. Cámaras corporales

En operaciones donde jurídicamente resulte apropiado y técnicamente viable, determinadas unidades podrán utilizar cámaras corporales. Su uso requerirá reglas sobre:

a) Inicio y finalización de grabación;

b) Privacidad;

c) Conservación;

d) Acceso;

e) Cadena de custodia;

f) Investigación administrativa;

g) Casos donde no proceda grabar.

La finalidad será proteger simultáneamente al ciudadano y al funcionario.

16.15. Analítica anticorrupción

SIGFRO-RD podrá producir alertas administrativas ante patrones estadísticamente anormales.

Ejemplo:

Un funcionario presenta una tasa de anulación de alertas considerablemente superior al promedio de funcionarios con funciones equivalentes. La plataforma podrá generar "Revisión administrativa recomendada" No, "Funcionario corrupto"

16.16. Indicadores de anomalías

Podrán analizarse:

a) Liberaciones excepcionales;

b) Anulaciones de alertas;

c) Inspecciones excesivamente cortas;

d) Modificaciones posteriores;

e) Accesos fuera del turno;

f) Consultas sin evento relacionado;

g) Concentración reiterada de determinados operadores con determinados funcionarios;

h) Exportación masiva de información;

i) Reapertura recurrente de expedientes;

j) Operaciones realizadas desde terminales no habituales.

16.17. Supervisión de supervisores

Los funcionarios con mayor nivel de acceso deberán estar sometidos a mayor trazabilidad. El administrador de un sistema no podrá disponer de capacidad para borrar el registro de sus propias actuaciones.

16.18. Registros inalterables

Los registros críticos deberán utilizar mecanismos técnicos que dificulten o impidan modificaciones no autorizadas. Cuando deba corregirse información:

dato anterior / modificación / usuario / fecha / motivo.

El historial deberá permanecer disponible.

16.19. Auditoría interna

Las Unidades de Auditoría Interna correspondientes podrán utilizar información de SIGFRO-RD para desarrollar auditorías orientadas por riesgo. Esto permitirá pasar de auditoría exclusivamente posterior a auditoría preventiva y analítica.

16.20. Alertas de control interno

Determinadas anomalías podrán ser remitidas automáticamente a los órganos internos de control correspondientes. El sistema deberá evitar, sin embargo, que una denuncia o anomalía menor produzca automáticamente una acusación disciplinaria.

16.21. Canal de denuncias

Se deberá disponer de mecanismos seguros para recibir información sobre:

a) Sobornos;

b) Contrabando;

c) Trata;

d) Tráfico ilícito;

e) Corrupción;

f) Alteración de controles;

g) Complicidad administrativa.

Los canales podrán permitir confidencialidad o anonimato cuando el marco jurídico lo permita.

16.22. Denuncia versus alerta oficial

Una denuncia ciudadana no deberá convertirse automáticamente en una alerta restrictiva contra una persona. El proceso deberá ser:

denuncia / evaluación / validación institucional / alerta cuando corresponda

16.23. Protección de información

La identidad de denunciantes protegidos no deberá quedar expuesta a usuarios fronterizos ordinarios.

16.24. Transparencia pública compatible con seguridad

Podrán publicarse indicadores agregados sobre:

a) Mercancías procesadas;

b) Tiempos promedio;

c) Incautaciones oficiales;

d) Alertas administrativas;

e) Disponibilidad tecnológica;

f) Estadísticas de comercio;

g) Auditorías generales;

h) Ejecución presupuestaria.

No deberán publicarse datos que comprometan:

a) Rutas de patrullaje;

b) Ubicación exacta de sensores sensibles;

c) Investigaciones;

d) Identidades protegidas;

e) Vulnerabilidades de infraestructura.

16.25. Evaluación de integridad

Cada institución deberá evaluar periódicamente los procesos de mayor exposición a corrupción. La pregunta fundamental será:

"¿En qué punto todavía puede una persona alterar el resultado sin dejar evidencia?"

Cuando se identifique ese punto, deberá rediseñarse el proceso.

16.26. Resultado esperado

El propósito no será eliminar la discrecionalidad humana donde esta sea necesaria.

Será transformar discrecionalidad invisible en discrecionalidad motivada, registrada y auditable.

CAPÍTULO XVII

COMERCIO FRONTERIZO, PUERTOS SECOS Y LOGÍSTICA INTELIGENTE

17.1. Cambio conceptual

La frontera no debe funcionar únicamente como espacio de contención. También debe constituirse en una infraestructura económica organizada.

En febrero de 2026 el Poder Ejecutivo anunció el desarrollo de una red de puertos secos bajo régimen de zona franca y centros logísticos fronterizos, con una inversión privada anunciada superior a US$300 millones y con el propósito declarado de ordenar el comercio y fortalecer el desarrollo económico de la zona fronteriza.

Esta política propone integrar esa iniciativa directamente con SIGFRO-RD.

17.2. Marco legal

El modelo logístico deberá armonizarse principalmente con:

a) Ley núm. 168-21 General de Aduanas;

b) Ley núm. 30-24 sobre Centros Logísticos, Empresas Operadoras de Centros Logísticos y Empresas Operadoras Logísticas;

c) Ley núm. 8-90 sobre Fomento de Zonas Francas;

d) Ley núm. 12-21 sobre la Zona Especial de Desarrollo Integral Fronterizo;

e) Legislación tributaria;

f) Normativa sanitaria;

g) Normativa ambiental;

h) Normativa de transporte;

i) Legislación laboral;

j) Normativa municipal y territorial aplicable.

La Ley núm. 30-24 establece actualmente el marco específico de centros y operadores logísticos y creó el Consejo Nacional de Logística.

17.3. Puertos secos fronterizos

Los puertos secos deberán concebirse como instalaciones interiores donde puedan concentrarse procesos tales como:

a) Recepción;

b) Estacionamiento;

c) Declaración;

d) Inspección;

e) Almacenamiento;

f) Consolidación;

g) Desconsolidación;

h) Control sanitario;

i) Pesaje;

j) Escaneo;

k) Liberación;

l) Despacho.

Su localización definitiva deberá sustentarse en estudios técnicos de:

a) Flujo comercial;

b) Conectividad vial;

c) Disponibilidad territorial;

d) Impacto ambiental;

e) Seguridad;

f) Acceso a energía;

g) Telecomunicaciones;

h) Agua;

i) Potencial productivo.

17.4. Nodos prioritarios

Los principales pasos y corredores fronterizos deberán estudiarse como potenciales nodos de la red, particularmente alrededor de:

a) Dajabón;

b) Elías Piña;

c) Jimaní;

d) Pedernales;

Sin prejuzgar la ubicación definitiva de los puertos secos ni sustituir los estudios de factibilidad correspondientes.

17.5. Separación de flujos

Los centros deberán separar físicamente, cuando sea posible:

a) Vehículos de carga;

b) Pequeños comerciantes;

c) Pasajeros;

d) Transporte público;

e) Operaciones oficiales;

f) Mercancías de riesgo;

g) Cargas que requieran inspección sanitaria.

Esto reducirá congestionamientos y mejorará la seguridad.

17.6. Pre-registro

Las operaciones formales deberán poder iniciarse antes de la llegada.

El operador podrá remitir:

a) Datos de la carga;

b) Vehículo;

c) Conductor;

d) Documentos;

e) Declaración;

f) Autorizaciones;

g) Hora prevista.

17.7. Sistema de citas

El transporte de carga podrá utilizar turnos digitales. Esto permitirá:

a) Evitar filas innecesarias;

b) Distribuir tráfico;

c) Programar inspectores;

d) Mejorar la seguridad vial;

e) Reducir tiempos;

f) Planificar utilización de escáneres.

17.8. Zona de espera inteligente

Los camiones podrán disponer de áreas de espera fuera del punto inmediato de cruce.

SIGFRO-RD podrá indicar vehículo autorizado para aproximarse. Esto evitará largas concentraciones de camiones sobre carreteras y accesos.

17.9. Control de entrada al centro

La entrada podrá verificarse automáticamente mediante:

a) RFID;

b) Matrícula;

c) Identificación del conductor;

d) Código de operación;

e) Cita.

17.10. Pesaje

Las básculas deberán integrarse digitalmente. El peso no deberá introducirse manualmente cuando el equipo pueda transmitirlo directamente.

17.11. Escaneo

Las cargas seleccionadas para control no intrusivo deberán vincular automáticamente las imágenes obtenidas con:

a) Declaración;

b) Contenedor;

c) Vehículo;

d) Operador;

e) Inspector;

f) Evento.

17.12. Almacenamiento y trazabilidad

Los depósitos deberán poder registrar:

- Entrada
- Ubicación
- Movimientos
- Inspecciones
- Salida.

17.13. Cadena de frío

Los puertos secos vinculados con alimentos, medicamentos o productos perecederos deberán disponer, según demanda, de:

a) Cámaras refrigeradas;

b) Energía redundante;

c) Sensores de temperatura;

d) Alarmas;

e) Registro histórico;

f) Áreas sanitarias especializadas.

17.14. Precintos inteligentes

Cargas sometidas a controles especiales podrán utilizar precintos electrónicos. Cualquier apertura no autorizada podrá producir una alerta.

17.15. Zona franca

El régimen de zonas francas podrá utilizarse cuando el proyecto y las empresas cumplan las condiciones establecidas por la Ley núm. 8-90.

El Consejo Nacional de Zonas Francas confirma que ese régimen continúa regulado por dicha legislación.

17.16. Desarrollo fronterizo

La Ley núm. 12-21 ofrece incentivos específicos a empresas calificadas en:

a) Pedernales;

b) Independencia;

c) Elías Piña;

d) Dajabón;

e) Montecristi;

f) Santiago Rodríguez;

g) Bahoruco.

Los proyectos logísticos y productivos deberán evaluar de manera coordinada los incentivos legalmente disponibles sin crear duplicidades o beneficios incompatibles.

17.17. Pequeño comercio fronterizo

Una frontera moderna no debe diseñarse exclusivamente para grandes empresas. El pequeño comerciante legítimo deberá disponer de mecanismos de formalización progresiva. Podrán desarrollarse, dentro de la legislación aplicable:

a) Registro simplificado;

b) Identificación digital;

c) Educación comercial;

d) Pagos electrónicos;

e) Declaraciones simplificadas cuando legalmente procedan;

f) Historial de cumplimiento;

g) Espacios de comercialización organizados.

17.18. Mercados fronterizos

Los mercados deberán transformarse progresivamente en espacios:

a) Identificados;

b) Seguros;

c) Sanitariamente adecuados;

d) Digitalizados;

e) Trazables;

f) Fiscalizables.

En agosto de 2026 el Gobierno inició, dentro de su estrategia "Frontera Fuerte", la construcción del Mercado Nacional de Tilory precisamente con el objetivo declarado de modernizar un espacio históricamente informal, mejorar condiciones sanitarias y ordenar la actividad comercial.

17.19. Digitalización de cobros

La modernización de mercados deberá incluir:

a) Conectividad;

b) Pagos digitales;

c) Facturación cuando legalmente corresponda;

d) Terminales;

e) Educación financiera;

f) Seguridad de transacciones.

INDOTEL aprobó un proyecto especial denominado "Conectividad y digitalización de cobros en Mercado Fronterizo", lo que ofrece una infraestructura institucional con la cual esta política deberá coordinarse.

17.20. Ventanilla logística

El operador deberá poder conocer digitalmente:

a) Estado de documentos;

b) Inspecciones pendientes;

c) Pago;

d) Autorizaciones;

e) Turno;

f) Resultado.

La meta será reducir la necesidad de recorrer múltiples oficinas físicas.

17.21. Expediente único de operación

Una operación logística podrá vincular:

a) Empresa

b) Conducto

c) Vehículo

d) Carga

e) Declaración

f) Inspección

g) Pago

h) Autorización

i) Salida

17.22. Operador confiable

Los operadores con historial comprobado de cumplimiento podrán acceder a procedimientos más ágiles cuando el régimen aduanero lo permita. La facilitación no supondrá ausencia de control.

17.23. Estadísticas comerciales

La digitalización permitirá conocer con mayor precisión:

a) Qué se comercializa;

b) En qué cantidades;

c) Desde dónde;

d) Hacia dónde;

e) En qué épocas;

f) Con qué frecuencia.

Estos datos podrán servir para desarrollar políticas productivas fronterizas.

17.24. Comercio dominicano hacia Haití

Los centros logísticos no deberán concebirse exclusivamente como puntos de inspección.

Podrán convertirse en plataformas de exportación para productores dominicanos.

17.25. Centros de consolidación

Los pequeños productores podrán agrupar cargas para reducir costos de transporte y logística.

17.26. Plataformas de servicios

Alrededor de estos nodos podrán surgir:

a) Transporte;

b) Mantenimiento;

c) Restauración;

d) Hospedaje;

e) Almacenamiento;

f) Seguros;

g) Servicios financieros;

h) Empaque;

i) Refrigeración;

j) Transformación agroindustrial.

17.27. Prevención de enclaves aislados

Los puertos secos no deberán convertirse en infraestructuras desconectadas de las comunidades.

La planificación deberá establecer encadenamientos con:

a) Productores;

b) Pymes;

c) Municipios;

d) Centros de formación;

e) Empresas fronterizas.

17.28. Resultado esperado

La frontera económica deberá evolucionar desde informalidad, congestión y discrecionalidad hacia registro, logística, trazabilidad, inversión y empleo.

CAPÍTULO XVIII

SANIDAD, AGRICULTURA Y PROTECCIÓN AMBIENTAL FRONTERIZA

18.1. Concepto de bioseguridad fronteriza

Una frontera segura no es únicamente aquella que controla personas y mercancías. También debe impedir o reducir la entrada y propagación de:

a) Enfermedades;

b) Plagas;

c) Organismos invasores;

d) Productos contaminados;

e) Animales enfermos;

f) Vegetales prohibidos;

g) Sustancias que afecten ecosistemas;

h) Residuos peligrosos.

Se propone incorporar dentro de SIGFRO-RD un Componente Integrado de Bioseguridad Fronteriza.

18.2. Marco jurídico sanitario

La Ley núm. 42-01 General de Salud constituye uno de los fundamentos principales para las actuaciones de protección sanitaria y regulación de acciones dirigidas a hacer efectivo el derecho a la salud.

La política deberá además respetar las normas específicas emitidas por:

a) Ministerio de Salud Pública;

b) Ministerio de Agricultura;

c) Autoridades de sanidad animal;

d) Autoridades fitosanitarias;

e) Ministerio de Medio Ambiente y Recursos Naturales;

f) Dirección General de Aduanas;

g) Demás órganos competentes.

18.3. Control basado en riesgo

No toda persona, animal, vehículo o mercancía presenta el mismo riesgo sanitario. El sistema deberá utilizar información para determinar cuándo corresponde:

a) Inspección;

b) Muestreo;

c) Retención;

d) Desinfección;

e) Cuarentena;

f) Rechazo;

g) Remisión a laboratorio.

18.4. Vigilancia epidemiológica

Los puntos fronterizos principales deberán integrarse con los sistemas nacionales de vigilancia epidemiológica. Cuando exista una alerta sanitaria formalmente emitida, SIGFRO-RD podrá ajustar determinados protocolos.

18.5. Privacidad sanitaria

La información médica individual deberá tratarse con protección reforzada. No deberá permitirse el acceso indiscriminado de funcionarios de seguridad a expedientes clínicos. En muchos casos bastará una respuesta operacional como:

"Evaluación sanitaria requerida."

18.6. Infraestructura sanitaria fronteriza

Los pasos principales deberán disponer, según el riesgo y volumen de operaciones, de áreas para:

a) Evaluación;

b) Aislamiento temporal;

c) Primeros auxilios;

d) Toma de muestras;

e) Conservación de muestras;

f) Equipos de protección;

g) Desinfección.

18.7. Emergencias epidemiológicas

El sistema deberá poder activar protocolos extraordinarios ante eventos formalmente declarados. Estos protocolos serán temporales y proporcionales.

18.8. Sanidad vegetal

La protección agrícola resulta especialmente relevante.

En mayo de 2026 el Ministerio de Agricultura informó el reforzamiento de controles fronterizos en Elías Piña, incluyendo vigilancia fitosanitaria, inspección para impedir trasiego de productos prohibidos y medidas destinadas a evitar la entrada de plagas y enfermedades. SIGFRO-RD deberá integrar tecnológicamente este tipo de controles.

18.9. Listas sanitarias actualizadas

Los inspectores deberán disponer de información actualizada sobre:

a) Productos prohibidos;

b) Productos restringidos;

c) Certificaciones necesarias;

d) Plagas bajo vigilancia;

e) Enfermedades;

f) Regiones de riesgo;

g) Medidas temporales.

18.10. Validación automática

Cuando sea jurídicamente posible, el sistema podrá verificar electrónicamente:

a) Certificados;

b) Permisos;

c) Vigencias;

d) Empresas autorizadas;

e) Productos habilitados.

18.11. Sanidad animal

El sistema deberá contemplar procedimientos para:

a) Animales vivos;

b) Carne;

c) Productos de origen animal;

d) Alimentos para animales;

e) Material biológico;

f) Subproductos.

18.12. Cuarentena agropecuaria

Las instalaciones principales deberán evaluar la necesidad de disponer de zonas seguras para retener temporalmente productos o animales sometidos a revisión sanitaria.

18.13. Trazabilidad de muestras

Una muestra tomada deberá registrar:

mercancía → inspector → fecha → lugar → muestra → laboratorio → resultado → decisión.

18.14. Laboratorios

Los puntos de mayor actividad podrán disponer de capacidades básicas o mecanismos logísticos para trasladar muestras rápidamente hacia laboratorios acreditados.

18.15. Alertas automáticas sanitarias

Un resultado positivo relevante podrá generar alertas sobre:

a) Producto;

b) Importador;

c) Exportador;

d) Lote;

e) Procedencia;

f) Vehículo;

g) Operaciones relacionadas.

Siempre conforme al procedimiento legal correspondiente.

18.16. Protección ambiental

La Ley núm. 64-00 constituye el marco general dominicano para la protección del medio ambiente y los recursos naturales.

La tecnología fronteriza podrá apoyar al Ministerio de Medio Ambiente dentro de sus competencias.

18.17. Áreas protegidas

Las zonas fronterizas comprenden ecosistemas de gran sensibilidad.

La Ley núm. 202-04 tiene como objeto garantizar la conservación y preservación de las unidades que conforman el Sistema Nacional de Áreas Protegidas.

La infraestructura de vigilancia deberá considerar particularmente aquellas áreas fronterizas que formen parte del sistema protegido.

18.18. Monitoreo ambiental mediante sensores

Podrán utilizarse:

a) Cámaras;

b) Drones;

c) Imágenes satelitales;

d) Sensores;

e) Sistemas geográficos,

para detectar potencialmente:

a) Incendios;

b) Tala;

c) Extracción ilegal;

d) Cambios de cobertura vegetal;

e) Construcciones no autorizadas;

f) Daños en cuencas;

g) Movimientos dentro de zonas especialmente protegidas.

18.19. Detección de incendios

Las cámaras térmicas y sistemas satelitales podrán servir también para identificar focos de calor. Una alerta ambiental deberá remitirse a la institución competente.

18.20. Cuencas compartidas

Los ríos y cuencas fronterizas requieren atención especial. La política deberá promover monitoreo de:

a) Calidad del agua;

b) Sedimentación;

c) Deforestación;

d) Contaminación;

e) Extracción de materiales;

f) Cambios hidrológicos.

18.21. Protección de infraestructura natural

La frontera posee elementos cuya pérdida puede afectar simultáneamente:

- Seguridad
- Agricultura
- Agua
- Comunidades

Por ello, la protección ambiental deberá integrarse a la estrategia de seguridad territorial.

18.22. Residuos

Los puertos secos, mercados y centros logísticos deberán disponer de planes para:

a) Residuos sólidos;

b) Residuos orgánicos;

c) Sustancias contaminantes;

d) Desechos sanitarios;

e) Residuos de inspecciones.

18.23. Mercancías ambientales restringidas

SIGFRO-RD podrá integrar alertas sobre productos cuya entrada, salida o transporte requiera autorización ambiental.

18.24. Evaluación ambiental de infraestructura

Las nuevas obras deberán cumplir los procedimientos de evaluación ambiental que correspondan. La tecnificación no deberá utilizarse como argumento para eludir permisos ambientales.

18.25. Mapa ambiental fronterizo

La plataforma podrá disponer de capas que indiquen:

a) Áreas protegidas;

b) Cuencas;

c) Bosques;

d) Zonas de riesgo;

e) Recursos hídricos;

f) Infraestructura ambiental.

18.26. Coordinación interinstitucional

Un mismo evento podrá ser simultáneamente:

- Aduanero
- Sanitario
- Ambiental.

SIGFRO-RD permitirá abrir una misma actuación para diferentes autoridades sin obligarlas a crear registros totalmente desconectados.

18.27. Indicadores

Se medirán, entre otros:

a) Inspecciones sanitarias;

b) Productos retenidos;

c) Plagas detectadas;

d) Alertas fitosanitarias;

e) Animales inspeccionados;

f) Muestras procesadas;

g) Incendios detectados;

h) Eventos ambientales;

i) Tiempo de respuesta;

j) Resultados confirmados.

18.28. Resultado esperado

La frontera deberá evolucionar hacia un sistema capaz de proteger no solamente el territorio dominicano, sino también su población, producción agrícola, recursos naturales, ecosistemas.

CAPÍTULO XIX

DESARROLLO ECONÓMICO Y SOCIAL DE LA ZONA FRONTERIZA

19.1. Principio estratégico

La seguridad fronteriza no puede descansar indefinidamente sobre una lógica exclusivamente militar. Una frontera donde existen:

a) Empleo;

b) Empresas;

c) Educación;

d) Infraestructura;

e) Servicios;

f) Conectividad;

g) Actividad productiva formal, posee mejores condiciones para mantener presencia estable de población dominicana y fortalecer el control territorial.

19.2. Mandato constitucional

El artículo 10 de la Constitución declara de supremo y permanente interés nacional tanto la seguridad como el desarrollo económico, social y turístico de la Zona Fronteriza. En consecuencia seguridad fronteriza y desarrollo fronterizo no son políticas competidoras, son componentes del mismo mandato constitucional.

19.3. Ley núm. 12-21

La política deberá aprovechar plenamente la Zona Especial de Desarrollo Integral Fronterizo establecida mediante la Ley núm. 12-21. La legislación comprende:

a) Pedernales;

b) Independencia;

c) Elías Piña;

d) Dajabón;

e) Montecristi;

f) Santiago Rodríguez;

g) Bahoruco.

La ley dispone un régimen de incentivos destinado a estimular inversiones y generación de actividad económica en dichas provincias.

19.4. Complementariedad con políticas existentes

La presente propuesta no pretende sustituir programas de desarrollo fronterizo existentes. Deberá integrarlos.

En agosto de 2026 el Gobierno inició nuevas obras dentro de la estrategia denominada "Frontera Fuerte", combinando seguridad, infraestructura, mercados, conectividad vial y desarrollo económico.

Frontera Inteligente RD deberá funcionar como componente tecnológico y de modernización capaz de complementar esas inversiones.

19.5. Modelo de polos fronterizos

Se propone estructurar Polos Integrados de Desarrollo Fronterizo alrededor de los corredores económicos con mayor potencial. Cada polo podrá especializarse según sus características. Ejemplos de actividades:

a) Agroindustria;

b) Logística;

c) Zonas francas;

d) Turismo;

e) Agricultura;

f) Ganadería;

g) Energías renovables;

h) Manufactura;

i) Servicios;

j) Comercio.

19.6. Especialización territorial

No todas las provincias deberán recibir exactamente el mismo modelo.

La planificación deberá identificar ventaja local, infraestructura necesaria, capacitación, inversión y mercado.

19.7. Agroindustria fronteriza

La frontera posee potencial para desarrollar cadenas de valor alrededor de productos agrícolas y pecuarios. La política deberá estimular que una mayor proporción de la producción sea cultivada, procesada, empacada, almacenada, comercializada dentro de la propia región.

19.8. Encadenamiento con puertos secos

Los centros logísticos del Capítulo XVII deberán funcionar como canales de salida para productores fronterizos.

Ejemplo:

Productor → Centro de acopio → Procesamiento → Consolidación → Puerto seco → Mercado Nacional o Exportación.

19.9. Centros de acopio

Se podrán promover instalaciones para:

a) Recepción;

b) Clasificación;

c) Lavado;

d) Empaque;

e) Refrigeración;

f) Almacenamiento;

g) Consolidación.

19.10. Información de mercado

Los productores deberán disponer progresivamente de información sobre:

a) Precios;

b) Demanda;

c) Calidad;

d) Volúmenes;

e) Oportunidades de exportación;

f) Requisitos sanitarios.

19.11. Formación técnica

El despliegue tecnológico generará nuevas necesidades laborales. Entre ellas:

a) Técnicos de redes;

b) Operadores de drones;

c) Electricistas;

d) Técnicos de energía solar;

e) Mecatrónica;

f) Reparación electrónica;

g) Logística;

h) Refrigeración;

i) Ciberseguridad;

j) Analítica de datos;

k) Mantenimiento de sensores.

19.12. Prioridad de formación local

Cuando sea posible, INFOTEP, universidades, politécnicos y demás instituciones podrán desarrollar programas dirigidos específicamente a residentes de las provincias fronterizas. La política deberá procurar "Tecnología instalada en la frontera → técnicos formados en la frontera."

19.13. Empleo local

Los contratos de mantenimiento y operación podrán incorporar, dentro del marco legal aplicable, programas de capacitación y transferencia de conocimientos dirigidos a trabajadores dominicanos de la región.

19.14. Centros de mantenimiento

En lugar de enviar cada equipo averiado a Santo Domingo, deberá evaluarse la creación progresiva de capacidad técnica regional. Esto:

a) Reduce tiempos;

b) Genera empleos;

c) Mejora disponibilidad;

d) Crea conocimiento local.

19.15. Pymes fronterizas

Los grandes proyectos deberán promover encadenamientos con pequeñas y medianas empresas locales. Ejemplos:

a) Transporte;

b) Alimentación;

c) Limpieza;

d) Construcción;

e) Mantenimiento;

f) Hospedaje;

g) Servicios técnicos;

h) Empaque;

i) Logística.

19.16. Digitalización de pequeños negocios

Los programas podrán incluir:

a) Internet;

b) Pagos digitales;

c) Contabilidad básica;

d) Facturación;

e) Comercio electrónico;

f) Capacitación financiera.

19.17. Inclusión financiera

La expansión de actividades formales deberá acompañarse de acceso a:

a) Cuentas bancarias;

b) Medios de pago;

c) Microcrédito;

d) Seguros;

e) Financiamiento productivo.

19.18. Juventud fronteriza

Deberá establecerse una línea específica para jóvenes.

El propósito será crear alternativas económicas vinculadas con:

a) Tecnología;

b) Agricultura;

c) Logística;

d) Servicios;

e) Turismo;

f) Emprendimiento.

19.19. Participación de mujeres

Los programas de emprendimiento, formación y acceso al financiamiento deberán procurar igualdad de oportunidades y eliminar obstáculos discriminatorios.

19.20. Servicios públicos

No será sostenible atraer inversión hacia zonas donde falten:

a) Agua;

b) Energía;

c) Internet;

d) Salud;

e) Educación;

f) Carreteras;

g) Vivienda adecuada.

Por ello, la estrategia económica deberá coordinarse con inversión social.

19.21. Conectividad vial

Serán parte de la infraestructura económica las carreteras que comunican los polos fronterizos con:

a) Puertos;

b) Aeropuertos;

c) Mercados internos;

d) Centros urbanos,

19.22. Mercado interno dominicano

El desarrollo fronterizo no debe depender exclusivamente de Haití. Las empresas deben poder producir para:

a) Mercado dominicano;

b) Exportación regional;

c) Estados Unidos;

d) Caribe;

e) Otros destinos.

Esto reduce vulnerabilidad económica.

19.23. Turismo

Las provincias con potencial turístico deberán articular el desarrollo de:

a) Ecoturismo;

b) Turismo cultural;

c) Turismo comunitario;

d) Turismo de naturaleza;

e) Servicios complementarios, siempre respetando áreas protegidas y ordenamiento territorial.

19.24. Incentivos condicionados a resultados

Los incentivos públicos deben vincularse con resultados verificables. Entre ellos:

a) Inversión ejecutada;

b) Empleos creados;

c) Empleos mantenidos;

d) Producción;

e) Cumplimiento fiscal;

f) Cumplimiento laboral;

g) Cumplimiento ambiental.

19.25. Registro de inversiones

Podrá crearse un tablero interinstitucional de seguimiento, sin sustituir los registros oficiales, que muestre:

a) Proyecto;

b) Provincia;

c) Sector;

d) Inversión comprometida;

e) Inversión ejecutada;

f) Empleo prometido;

g) Empleo creado;

h) Estado.

19.26. Evaluación del impacto de incentivos

Periódicamente deberá responderse:

¿Cuántos empleos produjo cada incentivo?

¿Cuánta inversión adicional generó?

¿Cuánto tiempo permanecieron las empresas?

¿Qué encadenamientos locales surgieron?

19.27. Desarrollo y seguridad

SIGFRO-RD podrá generar información agregada para evaluar cómo la formalización económica afecta:

a) Contrabando;

b) Comercio irregular;

c) Empleo;

d) movilidad;

e) Actividad comercial.

Los datos personales deberán protegerse.

19.28. Permanencia poblacional

Una política fronteriza exitosa deberá procurar que vivir en la frontera no constituya una desventaja estructural. El objetivo será que existan condiciones reales para nacer, estudiar, trabajar, emprender, formar familia y permanecer en las provincias fronterizas si la persona así lo desea.

19.29. Indicadores de desarrollo

Se medirán:

a) Nuevas empresas;

b) Inversión privada;

c) Empleos;

d) Salarios;

e) Formalización;

f) Exportaciones;

g) Producción agroindustrial;

h) Pymes vinculadas;

i) Acceso a internet;

j) Formación técnica;

k) Participación laboral;

l) Evolución demográfica.

19.30. Resultado esperado

La frontera deberá dejar de percibirse únicamente como la periferia que el Estado debe vigilar para convertirse progresivamente en un territorio estratégico que el Estado protege, conecta y desarrolla.

CAPÍTULO XX

INFRAESTRUCTURA ENERGÉTICA Y TELECOMUNICACIONES

20.1. Principio fundamental

La frontera inteligente depende de dos recursos invisibles que son la energía y conectividad.

Por ello, energía y conectividad deberán considerarse infraestructura crítica de la política fronteriza.

20.2. Situación energética

El sistema eléctrico nacional continúa experimentando una expansión importante de demanda. En julio de 2026 se registraron nuevos máximos históricos, lo que refuerza la necesidad nacional de mejorar generación, transmisión, distribución y resiliencia.

En la propia provincia Independencia, ETED informó en agosto de 2026 que la infraestructura local incluye aproximadamente 41 kilómetros y 141 torres de transmisión, calificándola como estratégica para la estabilidad del servicio y el desarrollo económico de las comunidades fronterizas.

20.3. Diseño energético de SIGFRO-RD

Cada instalación deberá clasificarse según criticidad.

Ejemplo:

Nivel A — Crítica	Centro de mando, comunicaciones principales, bases de datos, puntos fronterizos esenciales.
Nivel B — Operacional	Torres, sensores, estaciones de drones, puestos secundarios.
Nivel C — Complementaria	Equipos cuya interrupción temporal no paraliza operaciones.

20.4. Fuentes múltiples

Las instalaciones críticas no deberán depender exclusivamente de una sola fuente. Podrán combinar:

a) Red eléctrica;

b) Generadores;

c) Energía solar;

d) Baterías;

e) UPS;

f) Microredes;

g) Otras soluciones técnicamente justificadas.

20.5. Autonomía energética

Cada instalación deberá tener una autonomía mínima definida mediante estudio de riesgo.

Ejemplo:

Un centro de mando nacional requerirá mayor autonomía que una cámara secundaria.

20.6. Microredes

Los puntos remotos podrán utilizar sistemas híbridos, es decir, solar + batería + red/generador. Esto puede reducir:

a) Consumo de combustible;

b) Necesidad de transporte;

c) Vulnerabilidad;

d) costos operacionales.

20.7. Energía solar

La disponibilidad solar de la región fronteriza representa una oportunidad significativa. Sin embargo, los sistemas deberán dimensionarse considerando:

a) Consumo real;

b) Clima;

c) degradación;

d) almacenamiento;

e) vandalismo;

f) mantenimiento.

20.8. Monitoreo energético

SIGFRO-RD deberá visualizar:

a) Fuente activa;

b) Batería;

c) Consumo;

d) Generador;

e) Combustible;

f) Fallas;

g) Temperatura;

h) Autonomía restante.

20.9. Alerta preventiva

El sistema deberá avisar antes de producirse una pérdida completa de energía.

20.10. Combustible

Los generadores deberán disponer de controles para impedir:

a) Robo;

b) Utilización no autorizada;

c) Falta de abastecimiento;

d) Deterioro del combustible.

El consumo podrá ser telemedido cuando resulte costo-efectivo.

20.11. Protección física

Transformadores, torres, paneles, baterías y otros elementos críticos deberán contar con protección adecuada. La preocupación por la seguridad de la infraestructura eléctrica fronteriza ya ha motivado acciones específicas de ETED y autoridades locales en 2026.

20.12. Mantenimiento

Cada instalación energética tendrá:

a) Responsable;

b) Calendario;

c) Historial;

d) Vida útil;

e) Repuestos;

f) Pruebas periódicas.

20.13. Telecomunicaciones

La frontera inteligente necesitará una arquitectura de comunicaciones multinivel. No deberá depender de un único operador ni de un único medio.

20.14. Fibra óptica

La fibra será el medio principal para instalaciones fijas de elevada capacidad cuando resulte viable. Deberá buscarse:

a) Redundancia;

b) Rutas físicas alternativas;

c) Protección;

d) Monitoreo;

e) Reparación rápida.

20.15. Rutas redundantes

Cuando sea posible, los centros críticos deberán contar con dos rutas físicamente diferentes. Un mismo accidente no deberá cortar simultáneamente ambas conexiones.

20.16. Radioenlaces

En zonas donde la fibra resulte difícil o como respaldo podrán utilizarse enlaces de radio autorizados.

20.17. Redes móviles

La infraestructura podrá aprovechar 4G, 5G, servicios móviles disponibles, siempre considerando cobertura, seguridad y criticidad.

20.18. Redes privadas

Para determinados sistemas críticos podrán evaluarse redes privadas o segmentos específicamente protegidos.

20.19. Comunicación satelital

En puntos remotos o como última línea de contingencia podrá utilizarse conectividad satelital. No deberá convertirse necesariamente en el medio principal cuando existan alternativas más seguras o económicas.

20.20. Radio operacional

Las unidades terrestres deberán conservar comunicaciones de radio independientes de la conectividad convencional de internet.

Esto es fundamental durante:

a) Desastres;

b) Apagones;

c) Ciberataques;

d) Fallos de operadores comerciales.

20.21. Interoperabilidad de radio

Las instituciones deberán poder coordinarse durante incidentes conjuntos sin necesidad de compartir indiscriminadamente todas sus redes internas.

20.22. Espectro radioeléctrico

INDOTEL conservará sus competencias regulatorias sobre telecomunicaciones y espectro conforme a la legislación vigente.

La política deberá coordinar cualquier necesidad especial de frecuencias con dicha institución.

20.23. Interferencias fronterizas

La ubicación limítrofe presenta retos particulares relacionados con interferencias transfronterizas. INDOTEL ha documentado históricamente problemas de interferencia de radiodifusión y telefonía en la zona y mecanismos de coordinación técnica con Haití.

Por tanto, los sistemas fronterizos deberán utilizar planificación de frecuencias especialmente cuidadosa.

20.24. Brecha digital

La conectividad tecnológica del proyecto también podrá generar beneficios para las comunidades.

El Plan Bianual 2025-2026 de INDOTEL identificó varias provincias fronterizas — incluyendo Monte Cristi, Independencia, Bahoruco, Pedernales y Elías Piña— entre las de menor conectividad del país.

La infraestructura estatal deberá procurar, cuando técnica y legalmente resulte posible, producir sinergias con programas destinados a cerrar esa brecha.

20.25. Mercado fronterizo conectado

El proyecto aprobado por INDOTEL para conectividad y digitalización de cobros en mercados fronterizos constituye un ejemplo de cómo infraestructura de telecomunicaciones puede servir simultáneamente a control + comercio + inclusión digital.

20.26. Torres compartidas

Cuando resulte técnicamente viable, distintas instituciones podrán compartir infraestructura física de torres evitando duplicaciones innecesarias.

Cada sistema conservará la segregación lógica y de seguridad correspondiente.

20.27. Centro de monitoreo de comunicaciones

La red deberá permitir conocer:

a) Enlace activo;

b) Ancho de banda;

c) Latencia;

d) pérdida de paquetes;

e) interrupciones;

f) degradación;

g) respaldo activo.

20.28. Conmutación automática

Cuando falle el enlace principal, determinadas instalaciones deberán cambiar automáticamente hacia un enlace alternativo.

20.29. Calidad de servicio

Los contratos deberán establecer niveles mínimos verificables de disponibilidad. No bastará contratar "servicio de internet". Deberán establecerse:

a) Disponibilidad;

b) Capacidad;

c) Latencia;

d) Tiempo máximo de reparación;

e) Redundancia;

f) Soporte.

20.30. Seguridad de telecomunicaciones

Todo enlace deberá cumplir las políticas de ciberseguridad establecidas en el Capítulo XV.

La existencia de conectividad no deberá abrir innecesariamente los dispositivos a internet público.

20.31. Sincronización horaria

Cámaras, sensores, drones, servidores y sistemas deberán mantener referencias horarias sincronizadas.

Esto será indispensable para reconstruir eventos.

20.32. Condiciones ambientales

Los equipos instalados en la frontera deberán soportar:

a) Calor;

b) Humedad;

c) Polvo;

d) Lluvia;

e) Vientos;

f) Descargas eléctricas;

g) Variaciones de energía

20.33. Inventario georreferenciado

Cada activo energético y de telecomunicaciones deberá estar registrado en un mapa técnico.

20.34. Repuestos críticos

Se deberán mantener inventarios mínimos regionales de:

a) Baterías;

b) Radios;

c) Fuentes;

d) Conectores;

e) Cámaras;

f) Equipos de red;

g) Componentes de fibra

20.35. Contratos de mantenimiento

Los contratos deberán incluir:

a) Tiempo máximo de respuesta;

b) Tiempo máximo de reparación;

c) Repuestos;

d) Actualización;

e) Disponibilidad;

f) Penalidades cuando correspondan.

20.36. Transferencia tecnológica

Los proveedores deberán capacitar progresivamente al personal dominicano cuando el objeto contractual lo permita.

El Estado no deberá quedar permanentemente dependiente de técnicos extranjeros para tareas ordinarias de mantenimiento.

20.37. Protección ante desastres

La infraestructura deberá diseñarse considerando:

a) Huracanes;

b) Inundaciones;

c) Terremotos;

d) Deslizamientos;

e) Incendios;

f) Crecidas de ríos.

20.38. Recuperación

Cuando una instalación quede destruida, deberán existir procedimientos para desplegar rápidamente:

a) Generadores móviles;

b) Torres portátiles;

c) Radios;

d) Enlaces satelitales;

e) Drones;

f) Centros móviles.

20.39. Indicadores

Se medirán:

a) Disponibilidad eléctrica;

b) Disponibilidad de comunicaciones;

c) Horas en respaldo;

d) Fallos;

e) Tiempo medio de reparación;

f) Consumo energético;

g) Porcentaje de nodos redundantes;

h) Fibra disponible;

i) Enlaces alternativos;

j) Estaciones fuera de servicio;

k) Cobertura.

20.40. Resultado esperado

La infraestructura energética y de comunicaciones deberá conseguir que la frontera inteligente pueda continuar funcionando:

- Cuando se interrumpa la electricidad;
- Cuando se corte una fibra;
- Cuando falle un proveedor;
- Cuando ocurra un desastre;
- Cuando exista un ataque cibernético.

El concepto final será:

energía redundante + comunicaciones redundantes + operación degradada + recuperación rápida.

CAPÍTULO XXI

GOBERNANZA Y RESPONSABILIDADES INSTITUCIONALES

21.1. Principio general

La Política Nacional para la Tecnificación y Gestión Integral de la Frontera Dominico-Haitiana deberá operar bajo un modelo de dirección estratégica común y ejecución institucional descentralizada. No se propone crear una superinstitución fronteriza que absorba competencias actualmente ejercidas por:

a) Ministerio de Defensa;

b) CESFRONT;

c) Dirección General de Migración;

d) Dirección General de Aduanas;

e) Dirección Nacional de Inteligencia;

f) Ministerio de Salud Pública;

g) Ministerio de Agricultura;

h) Ministerio de Medio Ambiente y Recursos Naturales;

i) OGTIC;

j) Centro Nacional de Ciberseguridad;

k) INDOTEL;

l) Otras entidades competentes.

La regla de gobernanza será "Coordinación común, competencia institucional preservada."

21.2. No creación de una nueva entidad autónoma

SIGFRO-RD no tendrá personalidad jurídica independiente.

No deberá convertirse en:

a) Nuevo ministerio;

b) Nueva dirección general;

c) Nuevo organismo autónomo;

d) Nueva estructura burocrática permanente.

Será un sistema interinstitucional.

Los recursos humanos continuarán perteneciendo a sus respectivas instituciones.

Los presupuestos serán ejecutados por los organismos legalmente responsables de cada componente.

21.3. Comisión Interinstitucional de Implementación

Se propone constituir mediante decreto una Comisión Interinstitucional para la Frontera Inteligente —CIFI—

La Comisión no tendrá personalidad jurídica, patrimonio propio ni nómina independiente. Tendrá como misión dirigir estratégicamente la implementación coordinada de esta política.

21.4. Integración

Se propone que participen permanentemente:

a) Ministerio de la Presidencia;

b) Ministerio de Defensa;

c) Ministerio de Hacienda y Economía;

d) Dirección General de Migración;

e) Dirección General de Aduanas;

f) CESFRONT;

g) OGTIC;

h) Centro Nacional de Ciberseguridad;

i) Ministerio de Agricultura;

j) Ministerio de Salud Pública;

k) Ministerio de Medio Ambiente y Recursos Naturales;

l) INDOTEL;

m) Ministerio de Relaciones Exteriores;

n) Ministerio de Industria, Comercio y Mipymes cuando los asuntos tratados involucren logística, comercio o desarrollo empresarial.

La Dirección Nacional de Inteligencia participará en aquellos asuntos que correspondan a sus atribuciones legales.

La Ley núm. 1-24 reconoce entre los ámbitos de interés de la inteligencia estatal diversas amenazas transnacionales, incluidos tráfico de armas, narcotráfico, ciberataques, crimen transnacional y flujos migratorios irregulares, particularmente relevantes en la zona fronteriza.

21.5. Presidencia y coordinación

Se recomienda que la coordinación estratégica interinstitucional sea encabezada por el Ministerio de la Presidencia, debido al carácter transversal del proyecto.

El Ministerio de Defensa tendrá liderazgo operacional en los componentes directamente vinculados con seguridad y protección territorial. De esta forma se evita confundir dirección general de política pública con mando operacional fronterizo.

21.6. Secretaría Técnica

La Secretaría Técnica deberá funcionar utilizando capacidades existentes del Estado. Se propone un esquema conjunto donde:

a) Ministerio de Defensa coordine los requerimientos operacionales;

b) CESFRONT aporte las necesidades específicas de terreno;

c) OGTIC coordine arquitectura digital, interoperabilidad y estándares;

d) CNCS establezca y supervise los lineamientos de ciberseguridad correspondientes;

e) Cada institución mantenga un responsable técnico de integración.

No deberá crearse una estructura administrativa independiente para realizar estas funciones.

21.7. Relación con el Gabinete de Innovación y Desarrollo Digital

La gobernanza tecnológica deberá coordinarse con el **Gabinete de Innovación y Desarrollo Digital —GIDD—**, mecanismo ya existente de coordinación de las políticas de transformación digital del Estado.

El GIDD está presidido por el Ministerio de la Presidencia y OGTIC ejerce su Dirección Ejecutiva.

Por ello, la arquitectura tecnológica de Frontera Inteligente RD no deberá crear una política digital paralela.

21.8. Comité Técnico de SIGFRO-RD

El Comité Técnico Interinstitucional establecido en el Capítulo VI permanecerá como brazo técnico de la implementación.

Sus funciones serán:

a) Definir estándares;

b) Coordinar integraciones;

c) Revisar arquitectura;

d) Evaluar interoperabilidad;

e) Coordinar pruebas;

f) Gestionar versiones;

g) Revisar incidentes técnicos;

h) Preparar recomendaciones para la Comisión Interinstitucional.

21.9. Autoridad funcional

SIGFRO-RD utilizará el principio de autoridad funcional del evento.

En consecuencia:

Materia	Autoridad principal
Seguridad fronteriza	Ministerio de Defensa/CESFRONT según competencias
Control migratorio	Dirección General de Migración
Aduanas	Dirección General de Aduanas
Inteligencia estratégica	DNI dentro de sus competencias
Salud	Ministerio de Salud Pública
Sanidad agropecuaria	Autoridades agropecuarias competentes

Materia	Autoridad principal
Medio ambiente	Ministerio de Medio Ambiente
Telecomunicaciones y espectro	INDOTEL
Arquitectura digital gubernamental	OGTIC
Ciberseguridad nacional	CNCS
Planificación e inversión pública	Ministerio de Hacienda y Economía

21.10. Actualización institucional

Debe señalarse que la Ley núm. 45-25 fusionó los antiguos ministerios de Hacienda y de Economía, Planificación y Desarrollo y creó el actual Ministerio de Hacienda y Economía.

Esta institución concentra actualmente política fiscal, presupuesto y planificación e inversión pública, entre otras funciones.

Consecuentemente, toda referencia operativa futura de este Documento Marco deberá entenderse actualizada conforme a esa estructura.

21.11. Ministerio de Defensa

Tendrá, dentro de sus atribuciones:

a) Definir requerimientos de vigilancia territorial;

b) Coordinar operaciones militares;

c) Integrar capacidades del C5i;

d) Establecer prioridades operacionales;

e) Coordinar despliegue de sensores y drones relacionados con seguridad;

f) Gestionar comunicaciones militares;

g) Coordinar respuesta frente a amenazas fronterizas.

21.12. CESFRONT

CESFRONT conservará sus responsabilidades derivadas de los Decretos núm. 325-06 y 323-07.

El Decreto núm. 323-07 le asigna funciones relacionadas con dispositivos especializados de seguridad y control en puntos formales de entrada y salida y patrullaje complementario en la franja fronteriza. Su experiencia operacional deberá utilizarse para determinar:

a) Ubicación de sensores;

b) Necesidades de patrullaje;

c) Puntos críticos;

d) Tiempos de respuesta;

e) Requerimientos de centros de mando;

f) Necesidades de capacitación.

21.13. Dirección General de Migración

Será responsable de:

a) Sistemas migratorios;

b) Validación documental;

c) Biometría migratoria;

d) Entrada y salida;

e) Gestión de alertas migratorias;

f) Procedimientos secundarios;

g) Aplicación de la Ley núm. 285-04 y su reglamento.

21.14. Dirección General de Aduanas

Será responsable de:

a) Gestión aduanera;

b) SIGA;

c) IVF-RD;

d) Análisis de riesgo aduanero;

e) Declaraciones;

f) Inspecciones;

g) Fiscalización de cargas;

h) Sistemas de trazabilidad aduanera.

21.15. OGTIC

OGTIC tendrá responsabilidad técnica sobre:

a) Estándares digitales;

b) Interoperabilidad;

c) APIs gubernamentales;

d) Arquitectura tecnológica común;

e) NORTIC;

f) Servicios digitales compartidos;

g) Infraestructura gubernamental de nube cuando resulte aplicable;

h) Gobernanza tecnológica.

Actualmente OGTIC ofrece servicios gubernamentales de interoperabilidad, Firma GOB, nube gubernamental y asistencia técnica en transformación digital.

21.16. CNCS

El Centro Nacional de Ciberseguridad coordinará, dentro de sus competencias:

a) Lineamientos de seguridad;

b) Manejo de incidentes;

c) Coordinación con CSIRT-RD;

d) Evaluaciones de riesgo;

e) Protección de infraestructura crítica;

f) Ejercicios de ciberseguridad.

21.17. Ministerio de Hacienda y Economía

Será responsable, dentro de sus competencias, de:

a) Integración de la política con planificación nacional;

b) Registro y evaluación de proyectos de inversión pública;

c) Coordinación presupuestaria;

d) Análisis de sostenibilidad fiscal;

e) Evaluación económica;

f) Seguimiento de inversión;

g) Financiamiento público.

El Ministerio es actualmente órgano rector tanto de las finanzas públicas como del sistema nacional de planificación e inversión pública.

21.18. Organismos constitucionalmente autónomos

Instituciones constitucionalmente autónomas o independientes no deberán quedar subordinadas a la Comisión. Cuando SIGFRO-RD requiera interoperabilidad o colaboración con dichas instituciones, deberán utilizarse:

a) Convenios;

b) Protocolos;

c) Instrumentos jurídicos;

d) Mecanismos constitucionalmente válidos.

Esto será especialmente relevante respecto de organismos como:

a) Junta Central Electoral;

b) Ministerio Público;

c) Cámara de Cuentas,

21.19. Gobiernos locales

Dentro de sus competencias, los ayuntamientos de municipios fronterizos deberán participar en materias relacionadas con:

a) Ordenamiento local;

b) Mercados;

c) Residuos;

d) Tránsito;

e) Desarrollo urbano;

f) Actividades económicas municipales;

g) Protección civil;

21.20. Sector privado

Los operadores privados podrán participar mediante:

a) Contrataciones;

b) Concesiones o mecanismos jurídicamente procedentes;

c) Alianzas público-privadas;

d) Prestación de servicios;

e) Inversión logística;

f) Zonas francas.

Sin embargo, las funciones soberanas de autorización, coerción, inteligencia y decisión pública permanecerán bajo control del Estado.

21.21. Academia

Universidades, ITLA, INFOTEP y otros centros podrán colaborar en:

a) Formación;

b) Investigación;

c) Ciberseguridad;

d) Analítica;

e) Inteligencia artificial;

f) Mantenimiento tecnológico;

g) Evaluación.

21.22. Reuniones de gobernanza

La Comisión deberá reunirse Ordinariamente con periodicidad establecida y extraordinariamente ante eventos relevantes. No será necesario que todos los organismos participen en cada reunión técnica.

21.23. Matriz RACI

Cada proyecto deberá identificar:

R Responsable de ejecutar.

A Autoridad que aprueba.

C Institución consultada.

I Institución informada.

Ningún componente deberá comenzar sin esta definición.

21.24. Resolución de conflictos

Cuando existan discrepancias institucionales sobre datos, procesos, estándares, competencias, deberán agotarse mecanismos técnicos y jurídicos antes de elevar la controversia al nivel político correspondiente.

21.25. Principio de no duplicación

Antes de autorizar cualquier componente deberá responderse ¿Existe ya un sistema estatal capaz de realizar esta función? Si la respuesta es sí integrar antes que comprar**.**

21.26. Rendición de cuentas

Cada organismo deberá rendir cuentas sobre recursos recibidos, proyectos, hitos, indicadores, fallas, contrataciones y resultados.

21.27. Resultado esperado

La gobernanza deberá conseguir que múltiples instituciones puedan actuar:

"como un sistema coordinado, sin convertirse en una sola institución."

CAPÍTULO XXII

FINANCIAMIENTO Y MODELO DE IMPLEMENTACIÓN

22.1. Principio fiscal

La tecnificación fronteriza deberá concebirse como una inversión plurianual.

No deberá financiarse mediante adquisiciones aisladas efectuadas por diferentes organismos sin una arquitectura común. La secuencia deberá ser:

planificación → priorización → inversión → implementación → operación → mantenimiento → reposición.

22.2. Sistema Nacional de Planificación e Inversión Pública

Los proyectos que constituyan inversión pública deberán cumplir los procedimientos establecidos dentro del Sistema Nacional de Planificación e Inversión Pública.

La Ley núm. 498-06 creó dicho sistema precisamente para vincular las prioridades públicas con planes, programas, proyectos y presupuesto.

Las competencias correspondientes están hoy integradas al Ministerio de Hacienda y Economía como resultado de la Ley núm. 45-25.

22.3. Presupuesto General del Estado

Los componentes financiados directamente por el Gobierno deberán incluirse en las programaciones y presupuestos correspondientes.

La Ley núm. 423-06 establece el sistema presupuestario y persigue que la asignación y utilización de recursos públicos se realice eficaz y eficientemente para cumplir las políticas y objetivos estatales.

22.4. Integración financiera

La Ley núm. 5-07 establece que presupuesto, crédito público, tesorería y contabilidad forman parte del Sistema Integrado de Administración Financiera del Estado y exige vinculación entre planificación y presupuesto.

La política fronteriza deberá respetar esa estructura.

22.5. Programa Presupuestario Plurianual

Se recomienda estructurar un programa plurianual denominado, conceptualmente:

Programa Nacional de Frontera Inteligente

Este programa permitirá identificar separadamente:

a) Infraestructura;

b) Tecnología;

c) Comunicaciones;

d) Seguridad;

e) Capacitación;

f) Mantenimiento;

g) Reposición;

h) Ciberseguridad.

22.6. Presupuesto por componentes

No deberá existir únicamente un monto global. Cada inversión deberá clasificarse.

Ejemplo:

Componente	CAPEX	OPEX
Fibra y telecomunicaciones	Sí	Sí
Cámaras y sensores	Sí	Sí
Drones	Sí	Sí
Centros de mando	Sí	Sí
Software	Sí	Sí
Licencias	Según modelo	Sí
Ciberseguridad	Sí	Sí
Formación	Puede aplicar	Sí
Mantenimiento	No principalmente	Sí
Reposición	Sí	Programable

22.7. Costo total de propiedad

La comparación de tecnologías deberá considerar el Costo Total de Propiedad —TCO—. No deberá seleccionarse un equipo únicamente por su precio inicial. El TCO deberá incorporar:

a) Adquisición;

b) Instalación;

c) Licencias;

d) Conectividad;

e) Electricidad;

f) Mantenimiento;

g) Baterías;

h) Repuestos;

i) Almacenamiento;

j) Soporte;

k) Cpacitación;

l) Actualización;

m) Ciberseguridad;

n) Reemplazo;

o) Desmantelamiento

22.8. Horizonte de costo

Los proyectos tecnológicos críticos deberán evaluar costos de ciclo de vida, preferiblemente sobre horizontes de varios años. Un sistema aparentemente económico puede resultar extraordinariamente costoso si depende de:

a) Licencias anuales elevadas;

b) Repuestos exclusivos;

c) Servidores externos;

d) Consultoría permanente;

e) Mantenimiento propietario.

22.9. Fondo de reposición tecnológica

Cada componente deberá prever desde el inicio su eventual sustitución. La política no deberá reproducir el modelo:

comprar → inaugurar → utilizar → deteriorar → abandonar

Debe aplicarse:

comprar → operar → mantener → actualizar → reemplazar

22.10. Fuentes de financiamiento

Podrán utilizarse, según la naturaleza jurídica de cada proyecto:

a) Presupuesto General del Estado;

b) Inversión pública plurianual;

c) Financiamiento externo legalmente autorizado;

d) Cooperación internacional;

e) Donaciones;

f) Alianzas público-privadas para componentes apropiados;

g) Inversión privada directa en centros logísticos o zonas francas;

h) Otros mecanismos permitidos por legislación.

22.11. Crédito público

Todo financiamiento que constituya endeudamiento público deberá sujetarse al régimen legal correspondiente y a la Ley núm. 6-06 de Crédito Público. No deberá contraerse deuda tecnológica sin considerar:

a) Vida útil del activo;

b) Costo financiero;

c) Moneda;

d) Mantenimiento;

e) Riesgo cambiario;

f) Sostenibilidad fiscal

22.12. Alianzas público-privadas

Determinados componentes comercialmente explotables podrán evaluarse bajo la Ley núm. 47-20. La DGAPP continúa identificando esta ley como marco vigente para las APP, mientras la modificación anunciada durante 2026 permanece como proceso de reforma legislativa mientras no sea promulgada una norma sustituta.

Entre los sectores previstos por el modelo APP dominicano figuran telecomunicaciones, comercio internacional, infraestructura, energía, seguridad ciudadana y defensa nacional.

22.13. Componentes potencialmente aptos para APP

Podrían evaluarse:

a) Puertos secos;

b) Centros logísticos;

c) Almacenamiento;

d) Infraestructura energética;

e) Determinados servicios de telecomunicaciones;

f) Infraestructura comercial

22.14. Componentes que deberán permanecer bajo dominio estatal

Aunque proveedores privados puedan construir o mantener tecnología, deberán permanecer bajo control estatal:

a) Decisión migratoria;

b) Decisión aduanera;

c) Uso de fuerza;

d) Inteligencia;

e) Bases sensibles;

f) Claves criptográficas críticas;

g) Administración de alertas;

h) Decisiones coercitivas;

i) Mando operacional.

22.15. Fideicomiso público

La Ley núm. 28-23 regula actualmente el fideicomiso público dominicano. Su utilización deberá ser excepcional y sustentarse en un estudio que demuestre ventajas reales. No deberá utilizarse como mecanismo para:

a) Disminuir transparencia;

b) Fragmentar presupuesto;

c) Evitar controles;

d) Eludir reglas de contratación

22.16. Contrataciones públicas

Las adquisiciones deberán cumplir la Ley núm. 47-25 de Contrataciones Públicas, vigente desde el 28 de enero de 2026, así como su Reglamento aprobado mediante Decreto núm. 52-26 y demás normativa aplicable.

22.17. Contratación por resultados

Cuando sea legalmente procedente, los contratos tecnológicos deberán vincular pagos a hitos verificables.

Ejemplo:

- 20 % entrega.
- 20 % instalación.
- 20 % integración.
- 20 % pruebas.
- 20 % aceptación definitiva.

Los porcentajes concretos deberán definirse en cada contrato.

22.18. Prueba antes de aceptación

Ningún sistema deberá considerarse recibido únicamente porque el proveedor "lo instaló". Deberá comprobarse:

a) Funciona;

b) Se integra;

c) Soporta carga;

d) Cumple ciberseguridad;

e) Cumple documentación;

f) Cumple disponibilidad;

g) Fue probado en condiciones reales.

22.19. Garantía

Las contrataciones deberán prever:

a) Garantía;

b) Soporte;

c) Tiempo de respuesta;

d) Disponibilidad de piezas;

e) Actualizaciones;

f) Corrección de vulnerabilidades.

22.20. Propiedad de datos

Todo contrato deberá establecer expresamente:

"Los datos producidos en ejercicio de funciones públicas pertenecen y permanecen bajo control del Estado dominicano conforme al ordenamiento jurídico."

El proveedor no podrá utilizarlos comercialmente.

22.21. Portabilidad

El Estado deberá poder migrar sus datos hacia otro sistema. Se evitará el vendor lock-in. Los contratos deberán prever:

a) Exportación;

b) Formatos documentados;

c) APIs;

d) Documentación;

e) Procedimiento de salida

22.22. Código desarrollado a medida

Cuando el Estado financie software específicamente desarrollado para SIGFRO-RD, los contratos deberán determinar claramente:

a) Derechos de utilización;

b) Acceso al código cuando corresponda;

c) Documentación;

d) Posibilidad de modificación;

e) Continuidad ante desaparición del proveedor.

22.23. Transferencia tecnológica

Los contratos relevantes deberán incluir capacitación de personal dominicano. La meta será reducir progresivamente dependencia externa.

22.24. Compras consolidadas

Cuando varias instituciones necesiten equipos equivalentes, deberá evaluarse compra consolidada o estandarización cuando el régimen de contratación lo permita.

22.25. Prohibición de compras incompatibles

Ninguna institución deberá adquirir un sistema fronterizo relevante sin comprobar:

a) Compatibilidad;

b) Interoperabilidad;

c) Ciberseguridad;

d) Arquitectura;

e) Presupuesto operativo.

22.26. Autorización técnica

Los proyectos TIC deberán cumplir las revisiones y autorizaciones gubernamentales aplicables. OGTIC mantiene actualmente servicios específicos de asistencia técnica y autorización de compras TIC.

22.27. Cooperación internacional

La República Dominicana podrá recibir cooperación en:

a) Equipamiento;

b) Formación;

c) Sanidad;

d) Migración;

e) Aduanas;

f) Ciberseguridad;

g) Medio ambiente;

h) Gestión de desastres.

Toda cooperación deberá ajustarse a las prioridades tecnológicas dominicanas.

22.28. Donaciones tecnológicas

No deberá aceptarse automáticamente todo equipo ofrecido gratuitamente. Antes deberá determinarse:

a) Compatibilidad;

b) Seguridad;

c) Mantenimiento;

d) Repuestos;

e) Dependencia;

f) Vida útil;

g) Costo posterior.

Un equipo gratuito puede convertirse en una obligación costosa.

22.29. Transparencia financiera

Se recomienda publicar un tablero financiero con información no sensible sobre:

a) Proyecto;

b) Institución;

c) Proveedor;

d) Monto;

e) Avance financiero;

f) Avance físico;

g) Fecha;

h) Estado.

22.30. Comparación físico-financiera

SIGFRO-RD deberá relacionar **dinero ejecutado** con **resultado instalado.**

Ejemplo:

- Ejecución financiera: 80 %. Sensores funcionales: 35 %.

Esto deberá producir automáticamente una alerta de gestión.

22.31. Regla de sostenibilidad

Ningún nuevo componente deberá autorizarse sin identificar quién financiará:

a) Operación;

b) Mantenimiento;

c) Licencias;

d) Energía;

e) Conectividad;

f) Reemplazo

22.32. Resultado esperado

El modelo financiero deberá transformar compras tecnológicas aisladas en "inversión pública planificada, medible y sostenible durante todo el ciclo de vida."

CAPÍTULO XXIII

INDICADORES, AUDITORÍA Y EVALUACIÓN DE RESULTADOS

23.1. Principio general

Una política tecnológica no debe evaluarse por cantidad de cámaras compradas, drones adquiridos o kilómetros anunciados. Debe evaluarse por resultados verificables.

23.2. Línea base

Durante la etapa inicial se levantará una línea base nacional. Deberá determinar, como mínimo:

a) Infraestructura disponible;

b) Cobertura;

c) Tiempos de respuesta;

d) Capacidad migratoria;

e) Capacidad aduanera;

f) Conectividad;

g) Disponibilidad tecnológica;

h) Fallas;

i) Volumen de operaciones;

j) Costos;

k) Indicadores de desarrollo.

Sin línea base no será posible determinar objetivamente si la política produjo mejoras.

23.3. Indicadores de seguridad

Se medirán:

a) Tiempo medio desde detección hasta validación;

b) Tiempo medio desde validación hasta despacho;

c) Tiempo medio de llegada;

d) Porcentaje de eventos con cierre documentado;

e) Disponibilidad de sensores;

f) falsas alarmas;

g) Sectores con cobertura;

h) Eventos confirmados por múltiples sensores.

23.4. Indicadores migratorios

Se medirán:

a) Tiempo promedio de procesamiento;

b) Porcentaje de verificaciones biométricas exitosas;

c) Porcentaje de casos enviados a revisión secundaria;

d) Errores biométricos;

e) Duplicidades;

f) Incidencias de equipos;

g) Registros incompletos de entrada o salida según régimen aplicable.

23.5. Indicadores aduaneros

Se medirán:

a) Tiempo promedio de despacho;

b) Porcentaje de operaciones con información anticipada;

c) Operaciones inspeccionadas;

d) Diferencias de peso detectadas;

e) Utilización de controles no intrusivos;

f) Tiempos de inspección;

g) Disponibilidad de escáneres;

h) Operaciones de bajo riesgo procesadas.

23.6. Indicadores vehiculares

Se medirán:

a) Lecturas RFID;

b) Lecturas automáticas de matrículas;

c) Inconsistencias;

d) Etiquetas alteradas;

e) Tiempo de procesamiento;

f) Porcentaje de identificación automática.

23.7. Indicadores tecnológicos

Se medirán:

a) Uptime;

b) Tiempo medio entre fallas;

c) Tiempo medio de reparación;

d) Equipos fuera de servicio;

e) Mantenimiento cumplido;

f) Antigüedad;

g) Vulnerabilidades pendientes;

h) Conectividad.

23.8. Indicadores de drones

Se medirán:

a) Horas de vuelo;

b) Disponibilidad;

c) Misiones;

d) Eventos confirmados;

e) Falsas alertas descartadas;

f) Tiempo de respuesta aérea;

g) Incidentes;

h) Accidentes;

i) Costo por hora.

23.9. Indicadores de ciberseguridad

Se medirán:

a) Incidentes;

b) Intentos de intrusión;

c) Vulnerabilidades críticas;

d) Tiempo de detección;

e) Tiempo de contención;

f) Tiempo de recuperación;

g) Cumplimiento de parches;

h) Restauraciones exitosas de copias;

i) Accesos privilegiados;

j) Incidentes de datos personales.

23.10. Indicadores de integridad

Podrán medirse:

a) Excepciones;

b) Anulaciones de alertas;

c) Reasignaciones;

d) Consultas sin evento asociado;

e) Accesos fuera de horario;

f) Hallazgos administrativos;

g) Tiempo de cierre de hallazgos;

h) Denuncias validadas.

23.11. Cuidado en la interpretación

Una mayor cantidad de detecciones no significa necesariamente que exista más delito.

Puede significar simplemente mejor capacidad de detección. Los indicadores deberán interpretarse conjuntamente.

23.12. Prohibición de incentivos perversos

No deberán fijarse incentivos individuales únicamente sobre:

a) Número de detenciones;

b) Número de incautaciones;

c) Cantidad de inspecciones.

Estos indicadores pueden generar conductas distorsionadas.

23.13. Indicadores económicos

Se medirán:

a) Empresas fronterizas;

b) Operadores formalizados;

c) Empleo;

d) Inversión;

e) Exportaciones;

f) Actividad logística;

g) Operaciones en puertos secos;

h) Participación de Pymes;

i) Tiempo logístico;

j) Digitalización de pagos.

23.14. Indicadores sanitarios

Se medirán:

a) Inspecciones;

b) Muestras;

c) Tiempo de laboratorio;

d) Productos retenidos;

e) Alertas;

f) Plagas detectadas;

g) Tiempo de respuesta.

23.15. Indicadores ambientales

Se medirán:

a) Eventos detectados;

b) Incendios;

c) Alertas de tala;

d) Afectaciones de cuencas;

e) Tiempo de respuesta;

f) Areas bajo monitoreo.

23.16. Indicadores de inteligencia artificial

Cada modelo deberá medir:

a) Precisión;

b) Falsos positivos;

c) Falsos negativos;

d) Alertas confirmadas;

e) Decisiones humanas que contradicen al algoritmo;

f) Sesgos identificados;

g) Deterioro del modelo.

23.17. Indicadores presupuestarios

Se comparará el avance financiero vs. avance físico vs. resultado funcional.

No bastará conocer cuánto dinero fue gastado.

23.18. Tablero nacional

La Comisión Interinstitucional dispondrá de un tablero consolidado. Podrá utilizar semáforos:

- Verde Dentro de objetivo.
- Amarillo Desviación.
- Rojo Incumplimiento relevante.

23.19. Tablero público

Se publicará una versión agregada y no sensible. Podrá mostrar:

a) Inversión;

b) Disponibilidad;

c) Avances;

d) Comercio;

e) Tiempos de servicios;

f) Proyectos;

g) Indicadores económicos.

No incluirá información que facilite eludir los controles fronterizos.

23.20. Control interno

La Contraloría General de la República y las Unidades de Auditoría Interna ejercerán las competencias que les atribuye el ordenamiento jurídico.

23.21. Control externo

La Ley núm. 18-24 de la Cámara de Cuentas creó el actual Sistema Nacional de Control y Fiscalización y reconoce a la Cámara de Cuentas como órgano superior del sistema de control externo sobre la utilización de recursos públicos.

Esta legislación deberá ser utilizada como referencia principal para la fiscalización externa del programa.

23.22. Auditoría tecnológica

Además de la auditoría financiera deberán existir:

a) Auditorías de arquitectura;

b) Auditorías de software;

c) Auditorías de interoperabilidad;

d) Auditorías de disponibilidad;

e) Auditorías de contratos tecnológicos.

23.23. Auditoría de ciberseguridad

Las evaluaciones deberán incluir:

a) Pruebas de penetración;

b) Revisión de accesos;

c) Configuraciones;

d) Segmentación;

e) Vulnerabilidades;

f) Recuperación.

Los resultados técnicos sensibles deberán clasificarse adecuadamente.

23.24. Auditoría de algoritmos

Los modelos de alto impacto deberán someterse periódicamente a:

a) Pruebas de precisión;

b) Análisis de sesgos;

c) Revisión de variables;

d) Evaluación de falsos positivos;

e) Evaluación de falsos negativos.

23.25. Auditoría de privacidad

Se revisará:

a) Quién consulta;

b) Para qué consulta;

c) Cuánto tiempo se conservan datos;

d) Quién exporta;

e) Qué información se comparte;

f) Cumplimiento de permisos.

23.26. Auditoría física

Se comprobará físicamente:

a) Cámara instalada;

b) Ubicación;

c) Funcionamiento;

d) Serial;

e) Inventario;

f) Garantía;

g) Mantenimiento.

Esto impedirá que el control se limite a documentos administrativos.

23.27. Muestreo sorpresivo

Las auditorías podrán realizar comprobaciones no anunciadas sobre:

a) Equipos;

b) Turnos;

c) Registros;

d) Inventarios;

e) Accesos;

f) Procedimientos.

23.28. Evaluación anual

La política deberá producir un Informe Anual de Frontera Inteligente. El informe incluirá:

a) Resultados;

b) Inversiones;

c) Indicadores;

d) Proyectos;

e) Problemas;

f) Incidentes;

g) Metas del próximo período.

23.29. Evaluación intermedia

Al completarse aproximadamente la mitad del período inicial de implementación deberá realizarse una evaluación integral independiente.

Esta determinará:

a) Qué funciona;

b) Qué debe modificarse;

c) Qué componentes deben suspenderse;

d) Dónde invertir adicionalmente.

23.30. Evaluación final

Al concluir la fase de despliegue nacional deberá efectuarse una evaluación de impacto.

23.31. Control social

La Ley núm. 18-24 reconoce también el control social dentro del Sistema Nacional de Control y Fiscalización.

La ciudadanía deberá disponer de información agregada suficiente para evaluar la ejecución de recursos públicos sin comprometer operaciones de seguridad.

23.32. Resultado esperado

La evaluación deberá permitir responder anualmente:

"¿Es hoy la frontera más controlada, más rápida, más transparente, más segura y económicamente más productiva que antes de esta política?"

CAPÍTULO XXIV

IMPLEMENTACIÓN POR FASES

24.1. Principio

La República Dominicana no deberá intentar desplegar simultáneamente todo SIGFRO-RD en aproximadamente 391 kilómetros de frontera.

Una implementación masiva sin pruebas elevaría:

a) Riesgo;

b) Costos;

c) Errores;

d) Incompatibilidades;

e) Fallas operacionales.

Se propone una ejecución inicial de aproximadamente cinco años, dividida en fases.

FASE 0

PREPARACIÓN E INVENTARIO

Meses 0 a 6

24.2. Objetivos

Durante esta fase se realizará:

a) Inventario tecnológico nacional;

b) Inventario de bases de datos;

c) Mapa de infraestructura;

d) Evaluación jurídica;

e) Arquitectura SIGFRO-RD;

f) Línea base;

g) Evaluación de ciberseguridad;

h) Análisis de brechas;

i) Estudio presupuestario;

j) Priorización geográfica.

24.3. Inventario físico

Se identificarán:

a) Cámaras;

b) Sensores;

c) Radares;

d) Drones;

e) Servidores;

f) Fibra;

g) Radios;

h) Torres;

i) Energía;

j) Centros de mando;

k) Equipos biométricos;

l) RFID;

m) Escáneres.

24.4. Estado

Cada activo deberá clasificarse:

- Operativo.
- Operativo con limitaciones.
- Fuera de servicio.
- Obsoleto.
- Sin integración.

24.5. Inventario de sistemas

Se documentará:

a) Propietario;

b) Proveedor;

c) Tecnología;

d) APIs;

e) Bases de datos;

f) Seguridad;

g) Licencias;

h) Usuarios;

i) Dependencias.

24.6. Diagnóstico jurídico

Se determinará exactamente qué componentes pueden ejecutarse:

a) Bajo legislación vigente;

b) Mediante decreto;

c) Mediante reglamento;

d) Mediante convenio;

e) Mediante modificación legislativa.

24.7. Producto de Fase 0

La fase concluirá con un Plan Maestro de Frontera Inteligente RD, que contenga arquitectura, presupuesto, cronograma y prioridades definitivas.

FASE I

PILOTO INTEGRADO

- Meses 7 a 18

24.8. Selección

Se seleccionarán uno o dos corredores fronterizos utilizando criterios objetivos:

a) Volumen;

b) Riesgo;

c) Infraestructura existente;

d) Comercio;

e) Conectividad;

f) Capacidad institucional;

g) Representatividad.

Dajabón y Jimaní deberán ser evaluados como candidatos naturales, sin sustituir el estudio técnico definitivo.

24.9. Componentes piloto

El piloto deberá integrar realmente:

a) Migración;

b) Aduanas;

c) CESFRONT;

d) Cámaras;

e) Biometría;

f) IVF-RD;

g) Sensores;

h) Centro de mando;

i) Interoperabilidad;

j) Ciberseguridad;

k) Trazabilidad de funcionarios.

24.10. Regla fundamental

El piloto no consistirá en instalar únicamente nueva tecnología. Deberá probar el proceso completo:

detección → identificación → consulta → decisión → actuación → auditoría.

24.11. Pruebas

Se probarán:

a) Carga;

b) Conectividad;

c) Ciberseguridad;

d) Contingencia;

e) Operación nocturna;

f) Fallo eléctrico;

g) Fallo de internet;

h) Interoperabilidad;

i) Respuesta humana;

j) Protección de datos.

24.12. Evaluación del piloto

Antes de expandirse deberá determinarse:

a) Qué funcionó;

b) Qué falló;

c) Cuánto costó;

d) Qué debe cambiarse.

No deberá extenderse nacionalmente un sistema cuyo piloto no haya demostrado resultados.

FASE II

EXPANSIÓN A LOS PRINCIPALES PUNTOS FRONTERIZOS

- Meses 19 a 36

24.13. Cobertura

Según el orden final determinado por planificación, la arquitectura validada se extenderá progresivamente hacia:

a) Dajabón;

b) Elías Piña;

c) Jimaní;

d) Pedernales,

24.14. Componentes

Se ampliarán:

a) Biometría;

b) IVF-RD;

c) Fibra;

d) Centros;

e) Sensores;

f) Drones;

g) Logística;

h) Sanidad;

i) Interoperabilidad.

24.15. Centros regionales

Durante esta etapa se fortalecerán los centros regionales de mando.

24.16. Puertos secos

Los proyectos de centros logísticos y puertos secos técnicamente viables podrán comenzar o continuar paralelamente, según sus propios procesos de inversión y contratación.

FASE III

COBERTURA TERRITORIAL INTELIGENTE

- Meses 37 a 48

24.17. Cambio de enfoque

Una vez modernizados los principales pasos, la prioridad se trasladará hacia las zonas entre ellos. Se ampliarán:

a) Sensores;

b) Cámaras;

c) Radares;

d) Drones;

e) Comunicaciones;

f) Patrullaje orientado por riesgo.

24.18. Cobertura diferenciada

No se instalará la misma cantidad de tecnología en cada kilómetro. Para determinar necesidades se utilizará:

riesgo + geografía + historial + accesibilidad

24.19. Integración ambiental

La cobertura territorial deberá incorporar progresivamente vigilancia de:

a) Incendios;

b) Areas protegidas;

c) Cuencas;

d) Infraestructura.

FASE IV

CONSOLIDACIÓN NACIONAL

- Meses 49 a 60

24.20. Objetivo

Durante esta fase se consolidarán:

a) Integraciones;

b) Mantenimiento;

c) Analítica;

d) IA;

e) Auditoría;

f) Indicadores;

g) Desarrollo económico;

h) Continuidad operacional.

24.21. Sustitución tecnológica

Los primeros equipos que hayan alcanzado obsolescencia deberán entrar ya en ciclos de reemplazo.

24.22. Evaluación nacional

Al finalizar los primeros cinco años deberá realizarse una evaluación completa.

24.23. Operación permanente

Después del despliegue la política no termina. Comienza su etapa permanente de:

operación → mantenimiento → mejora → actualización.

24.24. Mecanismo de "puerta de fase"

Ninguna fase deberá avanzar únicamente porque llegó una fecha. Cada transición requerirá comprobar:

a) Indicadores;

b) Presupuesto;

c) Seguridad;

d) Interoperabilidad;

e) Capacidad humana;

f) Resultados.

24.25. Semáforo de avance

Cada componente se clasificará:

- Verde — Listo para expansión.
- Amarillo — Requiere corrección.
- Rojo — Expansión suspendida.

24.26. Resultado esperado

La implementación gradual reducirá el riesgo de que el Estado realice una gran inversión tecnológica antes de descubrir problemas fundamentales. La regla será:

"Probar pequeño, corregir rápido y escalar únicamente lo que funciona."

CAPÍTULO XXV

REFORMAS LEGALES Y REGLAMENTARIAS NECESARIAS

25.1. Principio jurídico

La implementación de Frontera Inteligente RD no deberá comenzar suponiendo que todas las leyes dominicanas necesitan ser modificadas. La metodología correcta será:

norma vigente → identificar competencia → identificar vacío → determinar instrumento necesario.

El instrumento podrá ser:

a) Protocolo;

b) Resolución;

c) Convenio;

d) Reglamento;

e) Decreto;

f) Modificación legislativa;

g) Nueva ley, dependiendo de la materia.

25.2. Constitución

No se identifica inicialmente la necesidad de modificar la Constitución.

La política encuentra sustento en:

a) Soberanía;

b) Seguridad nacional;

c) Régimen fronterizo;

d) Desarrollo económico fronterizo;

e) Competencias de las Fuerzas Armadas;

f) Potestades administrativas del Estado.

Simultáneamente deberá respetar plenamente:

a) Intimidad;

b) Protección de datos;

c) Debido proceso;

d) Igualdad;

e) Derechos fundamentales.

25.3. Decreto inicial de política pública

Se recomienda que el Poder Ejecutivo pueda adoptar, dentro de sus competencias, un decreto que:

a) Declare la Política Nacional de Frontera Inteligente;

b) Establezca sus principios;

c) Reconozca SIGFRO-RD;

d) Cree la Comisión Interinstitucional sin personalidad jurídica;

e) Ordene inventario;

f) Ordene elaboración del Plan Maestro;

g) Disponga coordinación de sistemas del Poder Ejecutivo;

h) Asigne responsabilidades generales;

i) Establezca mecanismos de seguimiento.

25.4. Límites del decreto

El decreto no podrá:

a) Crear delitos;

b) Modificar derechos establecidos por ley;

c) Alterar competencias legales;

d) Imponer obligaciones a órganos constitucionalmente autónomos fuera de los mecanismos constitucionales correspondientes;

e) Crear categorías migratorias nuevas;

f) Modificar tributos.

Estas materias requerirán el instrumento jurídico correspondiente.

25.5. Ley General de Migración núm. 285-04

Deberá efectuarse un análisis específico para determinar si el marco vigente resulta suficiente para regular:

a) Registro biométrico fronterizo;

b) Controles automatizados;

c) Entrada y salida electrónica;

d) Modalidades especiales relacionadas con mercados binacionales;

e) Intercambio de determinados datos;

f) Conservación de registros.

Cuando el régimen vigente sea suficiente, deberá utilizarse reglamentación. Cuando no lo sea, deberá proponerse una modificación específica.

25.6. Reglamento de Migración

Muchas reglas operativas podrán desarrollarse mediante reforma o complementación reglamentaria sin modificar la ley. Podrían incluir:

a) Estándares biométricos;

b) Procedimientos secundarios;

c) Credenciales;

d) Contingencias;

e) Registro digital.

25.7. Ley General de Aduanas núm. 168-21

El marco aduanero actual ya incorpora elementos importantes de digitalización y gestión de riesgo. Por ello, el principio será:

"Reglamentar antes de reformar."

Solo deberán plantearse modificaciones cuando se identifique un vacío concreto.

25.8. Regulaciones aduaneras

Podrán desarrollarse reglas para:

a) RFID;

b) Precintos electrónicos;

c) Evidencia producida por sistemas;

d) Interoperabilidad;

e) Pesaje automático;

f) Inspección digital;

g) Expediente electrónico.

25.9. CESFRONT

Los Decretos núm. 325-06 y 323-07 deberán revisarse técnicamente para determinar si necesitan actualización respecto de:

a) Vigilancia electrónica;

b) Operación de sensores;

c) Drones;

d) Centros de mando;

e) Interoperabilidad;

f) Coordinación digital.

La finalidad no será ampliar arbitrariamente competencias, será actualizar herramientas para ejercer las competencias existentes.

25.10. Ley Orgánica de las Fuerzas Armadas

Inicialmente no se identifica necesidad de modificación general de la Ley núm. 139-13 únicamente para ejecutar esta política. Cualquier necesidad específica deberá fundamentarse técnicamente.

25.11. Dirección Nacional de Inteligencia

La Ley núm. 1-24 deberá respetarse íntegramente. SIGFRO-RD no deberá convertirse en mecanismo para evadir las limitaciones y garantías que regulan las actividades de inteligencia.

25.12. Protección de datos personales

La Ley núm. 172-13 deberá revisarse conjuntamente con el artículo 44 constitucional para determinar si el tratamiento fronterizo requiere reglas especiales adicionales.

Especial atención deberá prestarse a:

a) Datos biométricos;

b) Reconocimiento facial;

c) Interoperabilidad;

d) Decisiones automatizadas;

e) Períodos de conservación;

f) Derechos de corrección;

g) Accesos;

h) Transferencias.

25.13. Categoría especial de datos biométricos

Se recomienda que el futuro marco legal trate expresamente la biometría utilizada por SIGFRO-RD como información que requiere protección reforzada.

25.14. Decisiones automatizadas

Deberá establecerse legalmente el principio de que ninguna decisión estatal de alto impacto relacionada con deportación, detención, incautación, sanción, restricción equivalente, pueda fundamentarse exclusivamente en una salida algorítmica sin intervención de autoridad competente.

25.15. Inteligencia artificial

Se recomienda desarrollar una regulación específica para los modelos de IA de alto impacto utilizados por el sistema. Deberá incluir:

a) Registro de modelos;

b) Auditoría;

c) Versionado;

d) Precisión;

e) Revisión humana;

f) Prohibición de perfilamiento discriminatorio;

g) Trazabilidad.

25.16. Interoperabilidad

La NORTIC A4:2024 constituye actualmente una base importante para intercambio de información entre organismos gubernamentales y se encuentra activa como norma de interoperabilidad gubernamental.

SIGFRO-RD deberá utilizar este marco y el Marco Nacional de Interoperabilidad antes de desarrollar sistemas paralelos.

25.17. Convenios interinstitucionales

Cada integración sensible deberá establecer:

a) Datos;

b) Finalidad;

c) Autoridad;

d) Usuarios;

e) Seguridad;

f) Conservación;

g) Auditoría;

h) Procedimiento de incidentes.

25.18. Identificador Único de Evento Fronterizo

El futuro marco jurídico deberá reconocer la posibilidad de utilizar el IUEF como mecanismo de vinculación operacional entre instituciones.

Esto no sustituirá los números de expediente propios de:

a) Migración;

b) Aduanas;

c) Ministerio Público;

d) Tribunales;

e) Otras instituciones.

25.19. Registros electrónicos

Deberá garantizarse jurídicamente que:

a) Logs;

b) Sellos de tiempo;

c) Fotografías;

d) Videos;

e) Lecturas RFID;

f) Datos de sensores;

g) Registros de acceso, puedan conservarse con mecanismos adecuados de integridad y autenticidad.

25.20. Evidencia digital

La utilización procesal de estos registros deberá cumplir las normas dominicanas de evidencia y cadena de custodia.

La plataforma no deberá pretender sustituir mediante tecnología los requisitos procesales correspondientes.

25.21. Drones

Las operaciones deberán cumplir el marco aeronáutico aplicable y las disposiciones correspondientes del IDAC, incluyendo RAD 107 cuando resulte aplicable.

Las operaciones estatales especiales deberán disponer de protocolos que delimiten:

a) Autoridad;

b) Zonas;

c) Seguridad aérea;

d) Conservación de imágenes;

e) Actuación ante fallos;

f) Relación con espacio aéreo internacional.

25.22. Ciberseguridad

La regulación deberá armonizar SIGFRO-RD con:

a) Ley núm. 53-07;

b) Estrategia Nacional de Ciberseguridad 2030;

c) Lineamientos CNCS;

d) NORTIC de seguridad;

e) Protocolos CSIRT-RD.

25.23. Infraestructura crítica

Deberá evaluarse la inclusión formal de determinados componentes de SIGFRO-RD dentro del régimen nacional aplicable a infraestructuras críticas.

25.24. Contrataciones

No se recomienda crear un régimen general de contrataciones fronterizas separado.

Las adquisiciones deberán efectuarse conforme a la Ley núm. 47-25 y su Reglamento. Las excepciones relacionadas con seguridad nacional deberán utilizarse únicamente cuando la propia legislación las permita y se cumplan sus requisitos.

25.25. Control fiscal

La política deberá someterse plenamente al Sistema Nacional de Control y Fiscalización establecido por la Ley núm. 18-24.

25.26. Desarrollo fronterizo

La Ley núm. 12-21 deberá utilizarse como instrumento económico.

No se recomienda modificarla simplemente para crear nuevos incentivos sin demostrar previamente que los existentes son insuficientes.

25.27. Ley de APP

Las alianzas público-privadas que formen parte del proyecto deberán utilizar el régimen legal general vigente. No se recomienda crear una "APP fronteriza" especial.

25.28. Nuevo anteproyecto de ley

Luego del análisis jurídico completo, se considera conveniente elaborar un:

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

Este instrumento no deberá sustituir las leyes sectoriales existentes. Su función será proporcionar el marco transversal que actualmente ninguna ley sectorial cubre por sí sola.

25.29. Contenido recomendado del futuro anteproyecto

Deberá establecer:

a) Objeto;

b) Ambito de aplicación;

c) Principios;

d) Definición de Frontera Inteligente;

e) Reconocimiento jurídico de SIGFRO-RD;

f) Gobernanza interinstitucional;

g) Autoridad funcional;

h) Interoperabilidad;

i) IUEF;

j) Trazabilidad de funcionarios;

k) Protección de datos;

l) Biometría;

m) Inteligencia artificial;

n) Auditoría algorítmica;

o) Ciberseguridad;

p) Infraestructura crítica;

q) Continuidad operacional;

r) Evidencia digital;

s) Auditoría;

t) Indicadores;

u) Régimen de responsabilidad;

v) Implementación progresiva.

25.30. Manipulación del sistema

Deberá analizarse si el ordenamiento penal y disciplinario vigente cubre adecuadamente conductas como:

a) Alteración deliberada de una alerta;

b) Manipulación de registros;

c) Eliminación de evidencia;

d) Acceso ilegítimo;

e) Clonación de identificadores;

f) Sabotaje de sensores;

g) Manipulación de sistemas biométricos.

Solo cuando exista un vacío real deberán proponerse nuevas infracciones.

25.31. Responsabilidad de proveedores

Los contratos y, cuando proceda, la regulación deberán establecer responsabilidad frente a:

a) Vulnerabilidades ocultadas;

b) Accesos no autorizados;

c) Uso indebido de datos;

d) Incumplimiento de seguridad;

e) Pérdida de información;

f) Incumplimiento de niveles de servicio.

25.33. Consulta previa al anteproyecto

Antes de someter el proyecto legislativo deberán participar técnicamente:

a) Ministerio de Defensa;

b) CESFRONT;

c) Migración;

d) Aduanas;

e) OGTIC;

f) CNCS;

g) Ministerio de Hacienda y Economía;

h) Consultoría Jurídica del Poder Ejecutivo;

i) Salud Pública;

j) Agricultura;

k) Medio Ambiente;

l) INDOTEL;

m) Academia;

n) Especialistas en protección de datos;

o) Organizaciones empresariales fronterizas;

p) Comunidades fronterizas.

25.33. Revisión constitucional

Antes del sometimiento deberá realizarse una matriz que confronte cada disposición con:

a) Constitución;

b) Derechos fundamentales;

c) Reserva de ley;

d) Competencias institucionales;

e) Tratados aplicables.

25.34. Implementación jurídica escalonada

La secuencia recomendada será:

ETAPA 1	Utilizar plenamente las facultades ya existentes.
ETAPA 2	Emitir decreto de política pública y protocolos interinstitucionales.
ETAPA 3	Implementar piloto dentro de competencias vigentes.
ETAPA 4	Identificar vacíos jurídicos reales.
ETAPA 5	Someter el Anteproyecto de Ley de Gestión Integrada y Tecnificación Fronteriza.

Esto evita legislar sobre supuestos problemas antes de comprobar operacionalmente cuáles requieren realmente una solución legislativa.

25.35. Cláusula de revisión tecnológica

La futura legislación deberá evitar mencionar marcas, tecnologías propietarias o especificaciones que se vuelvan rápidamente obsoletas. Debe establecer principios funcionales.

25.36. Revisión periódica

La política y su normativa deberán revisarse periódicamente para adaptarse a:

a) Nuevas amenazas;

b) Nuevas tecnologías;

c) Cambios legales;

d) Evolución comercial;

e) Ciberseguridad;

f) Inteligencia artificial.

25.37. Resultado jurídico esperado

El ordenamiento resultante deberá permitir más capacidad estatal sin menos garantías constitucionales.

Tecnificar la frontera no significa reducir controles jurídicos, significa lograr que el Estado ejerza sus atribuciones con mayor precisión, mayor trazabilidad, mayor coordinación, mayor responsabilidad.

CONCLUSIÓN GENERAL

La República Dominicana enfrenta el desafío histórico de administrar una frontera terrestre extensa, compleja y estratégica en un contexto marcado simultáneamente por presiones migratorias, crimen transnacional, contrabando, comercio binacional, riesgos sanitarios, desafíos ambientales, desarrollo desigual de las provincias fronterizas y transformación tecnológica acelerada.

La respuesta no puede reducirse exclusivamente a más soldados, ni únicamente a más kilómetros de verja.

Ambos instrumentos pueden resultar necesarios dentro de una estrategia mayor.

La verdadera transformación consiste en lograr que la República Dominicana evolucione desde UNA FRONTERA VIGILADA hacia UNA FRONTERA GESTIONADA INTELIGENTEMENTE.

El modelo propuesto integra

INFRAESTRUCTURA FÍSICA	Verja, carreteras, torres, puestos y centros logísticos.
VIGILANCIA TECNOLÓGICA	Cámaras, sensores, radares y drones.
IDENTIDAD	Documentación, biometría y validaciones institucionales.
VEHÍCULOS	Matrícula, VIN, RFID e IVF-RD.
MERCANCÍAS	Declaración, peso, inspección y trazabilidad.
INTEROPERABILIDAD	Sistemas estatales comunicándose bajo competencias claramente delimitadas.
INTELIGENCIA	Correlación de eventos y análisis de riesgo.
INTELIGENCIA ARTIFICIAL	Tecnología que recomienda y prioriza, pero no sustituye a la autoridad.

CIBERSEGURIDAD	Protección permanente de infraestructura y datos.
INTEGRIDAD	Funcionario identificado, actuación registrada y decisión auditable.
ECONOMÍA	Puertos secos, mercados formalizados, logística y zonas productivas.
DESARROLLO	Empleo, capacitación, Pymes e inversión.
BIOSEGURIDAD	Protección sanitaria, agrícola y pecuaria.
MEDIO AMBIENTE	Cuencas, bosques, áreas protegidas y recursos naturales.
ENERGÍA Y CONECTIVIDAD	Infraestructura redundante capaz de mantener operativa la frontera.
CONTROL	Indicadores, auditoría interna, control externo y evaluación pública.