

ANTEPROYECTO DE LEY

SOBRE SEGURIDAD PENITENCIARIA INTEGRAL, TECNOLÓGICA Y DE COMUNICACIONES

EXPOSICIÓN DE MOTIVOS

El sistema penitenciario constituye una función esencial del Estado vinculada con la seguridad, la protección de las personas privadas de libertad, la integridad del personal, la custodia, la rehabilitación y la reinserción social. La evolución tecnológica ha creado nuevas oportunidades para la comunicación legítima, pero también nuevos riesgos cuando dispositivos de comunicación no autorizados son introducidos o utilizados dentro de los establecimientos penitenciarios.

La respuesta pública no debe descansar exclusivamente en decomisos o sanciones. Debe integrar prevención, control de acceso, detección, monitoreo, inteligencia, ciberseguridad, comunicaciones legítimas, capacitación, integridad institucional, investigación, evidencia digital, evaluación y continuidad operacional, respetando en todo momento la Constitución y el ordenamiento jurídico.

El presente anteproyecto establece un marco nacional de seguridad penitenciaria integral y tecnológicamente asistida. Su propósito es reducir las oportunidades de utilización clandestina de dispositivos de comunicación y fortalecer la capacidad institucional para detectar, contener, documentar e investigar incidentes, sin autorizar vigilancia indiscriminada, interceptaciones al margen de la ley ni tecnologías destinadas a dañar físicamente dispositivos o poner en riesgo a personas, instalaciones o servicios esenciales.

VISTOS

Vista: La Constitución de la República Dominicana, proclamada el 27 de octubre de 2024, en particular sus disposiciones relativas a la dignidad humana, los derechos fundamentales, la intimidad, el secreto de las comunicaciones, la tutela judicial efectiva, el debido proceso, la finalidad de la pena y las atribuciones de los poderes públicos.

Vista: La Ley núm. 113-21, que regula el Sistema Penitenciario y Correccional de la República Dominicana, con las modificaciones que se encuentren vigentes.

Vista: La Ley núm. 80-25, que crea el Ministerio de Justicia y establece disposiciones sobre su organización y competencias, incluidas las modificaciones que introduce al régimen penitenciario.

Vista: La Ley núm. 74-25, que instituye el Código Penal de la República Dominicana, modificada por la Ley núm. 44-26, con observancia de sus disposiciones de vigencia y transición.

Vista: La normativa procesal penal vigente, en cuanto regula la investigación penal, la obtención de pruebas, la autorización judicial y las garantías de las personas investigadas.

Vista: La Ley General de Telecomunicaciones núm. 153-98, y sus disposiciones reglamentarias vigentes, en lo relativo a las atribuciones del Instituto Dominicano de las Telecomunicaciones (INDOTEL).

Vista: La Ley núm. 172-13, sobre Protección de Datos de Carácter Personal, y demás normas aplicables al tratamiento y protección de información personal.

Vista: La Ley núm. 200-04, General de Libre Acceso a la Información Pública, y su normativa de aplicación.

Vista: La Ley núm. 41-08, de Función Pública, en lo concerniente a deberes, responsabilidades y régimen disciplinario del personal público.

Vista: La Ley núm. 47-25, de Contrataciones Públicas, y su Reglamento de Aplicación aprobado mediante el Decreto núm. 52-26, sin perjuicio de las reglas transitorias aplicables.

Vista: La Ley núm. 53-07, sobre Crímenes y Delitos de Alta Tecnología, en las materias que correspondan.

Vistos: Los tratados internacionales de derechos humanos ratificados por la República Dominicana, especialmente aquellos relativos al trato digno de las personas privadas de libertad y a las garantías judiciales.

CONSIDERANDOS

CONSIDERANDO: Que la seguridad de los establecimientos penitenciarios es una responsabilidad esencial del Estado y debe ejercerse de manera compatible con la dignidad humana, la legalidad, la finalidad de la pena y los derechos de las personas privadas de libertad.

CONSIDERANDO: Que la introducción y utilización de teléfonos celulares y otros dispositivos de comunicación no autorizados en centros penitenciarios pueden facilitar amenazas, extorsiones, fraudes, coordinación de actividades delictivas y otras conductas que ponen en riesgo a víctimas, familiares, personal penitenciario y a la sociedad.

CONSIDERANDO: Que la prevención de tales riesgos exige superar las respuestas aisladas y establecer un sistema integral de controles físicos, humanos, administrativos y tecnológicos, capaz de identificar vulnerabilidades, detectar incidentes y corregir sus causas.

CONSIDERANDO: Que la eficacia de la seguridad penitenciaria depende de procedimientos verificables para el ingreso y salida de personas, vehículos, bienes, paquetes, herramientas y equipos, así como de la trazabilidad de las autorizaciones y actuaciones institucionales.

CONSIDERANDO: Que la detección técnica de un dispositivo, su localización y la interceptación o acceso al contenido de una comunicación son actuaciones jurídicamente distintas, por lo que las medidas de control deberán sujetarse a las competencias, autorizaciones y garantías exigidas por el ordenamiento.

CONSIDERANDO: Que las comunicaciones legítimas con familiares, defensores y autoridades competentes, conforme a las garantías aplicables, contribuyen al mantenimiento de vínculos sociales, a la reinserción y a la reducción de incentivos para recurrir a medios clandestinos.

CONSIDERANDO: Que el fortalecimiento de la seguridad requiere sistemas de videovigilancia, monitoreo, registros, protección de infraestructura crítica, continuidad operacional y respuesta a incidentes, seleccionados conforme a su eficacia, seguridad, proporcionalidad y sostenibilidad.

CONSIDERANDO: Que la información y la evidencia digital obtenidas en actuaciones de seguridad deben gestionarse con criterios de integridad, confidencialidad, finalidad, minimización, trazabilidad y cadena de custodia, evitando accesos indebidos y usos incompatibles con la ley.

CONSIDERANDO: Que el uso de herramientas de análisis automatizado e inteligencia artificial puede contribuir a identificar anomalías y tendencias, pero no debe sustituir el juicio humano ni servir por sí solo para determinar responsabilidades o restringir derechos.

CONSIDERANDO: Que la corrupción, la complicidad interna, la omisión deliberada de controles y el acceso indebido de terceros constituyen riesgos institucionales que requieren medidas preventivas, auditorías, separación de funciones, capacitación y mecanismos seguros de denuncia.

CONSIDERANDO: Que la modernización tecnológica debe ejecutarse mediante adquisiciones transparentes y verificables, con criterios de interoperabilidad, mantenimiento, seguridad de la información, costo total de propiedad y prevención de dependencias injustificadas de proveedores.

CONSIDERANDO: Que la coordinación entre el Ministerio de Justicia, los órganos responsables de la administración penitenciaria, el Ministerio Público, el Poder Judicial, INDOTEL y las demás instituciones competentes debe respetar la distribución constitucional y legal de atribuciones.

CONSIDERANDO: Que ninguna solución tecnológica de seguridad puede justificar medidas indiscriminadas, métodos destructivos que comprometan la integridad de las personas o instalaciones, ni actuaciones de investigación o vigilancia al margen de la ley.

CONSIDERANDO: Que la profesionalización del personal, la evaluación periódica de resultados, la auditoría independiente cuando proceda y la rendición de cuentas constituyen condiciones indispensables para la efectividad y legitimidad de la política pública.

CONSIDERANDO: Que resulta necesario establecer un marco legal integral que articule prevención, detección, control, respuesta, coordinación institucional, protección de derechos, comunicaciones legítimas y mejora continua, y que permita su desarrollo mediante reglamentos y protocolos técnicos sujetos a la ley.

HA DADO LA SIGUIENTE LEY

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto. La presente ley establece los principios, objetivos y mecanismos generales para fortalecer la seguridad penitenciaria mediante un modelo integral de prevención, control físico, tecnológico, informacional y humano, con especial atención a la prevención y gestión del ingreso y uso de dispositivos de comunicación no autorizados.

Artículo 2.- Ámbito de aplicación. Las disposiciones serán aplicables, en el ámbito de las competencias legalmente atribuidas, a los establecimientos y servicios penitenciarios y correccionales administrados por el Estado, así como al personal, contratistas, proveedores, visitantes y terceros que desarrollen actividades dentro de dichos establecimientos.

Artículo 3.- Finalidades. Son finalidades de esta ley: 1) proteger la seguridad de los establecimientos; 2) prevenir la utilización clandestina de medios tecnológicos; 3) fortalecer la detección e investigación de incidentes; 4) proteger derechos fundamentales; 5) asegurar comunicaciones legítimas; 6) reducir riesgos de corrupción y complicidad; 7) fortalecer la continuidad operacional; y 8) promover evaluación permanente.

Artículo 4.- Principios. La aplicación de esta ley se regirá por legalidad, necesidad, proporcionalidad, prevención, dignidad humana, reinserción, seguridad, mínima intervención, responsabilidad, trazabilidad, protección de datos, seguridad de la información, neutralidad tecnológica, continuidad operacional, rendición de cuentas y mejora continua.

Artículo 5.- Definiciones básicas. Para los fines de esta ley se entenderá por dispositivo no autorizado todo equipo de comunicación, conectividad o tecnología que no haya sido autorizado conforme al régimen institucional aplicable; por detección la identificación técnica de la posible presencia o actividad de un dispositivo; por localización la determinación técnica aproximada de su ubicación; y por interceptación el acceso al contenido o captación de comunicaciones, actividad que solamente podrá realizarse cuando exista habilitación constitucional, legal y judicial cuando corresponda.

Artículo 6.- Interpretación conforme al ordenamiento vigente. Las disposiciones de esta ley se interpretarán de conformidad con la Constitución, la legislación penitenciaria vigente, la legislación penal y procesal penal, las normas sobre telecomunicaciones, protección de datos, función pública, contratación pública, archivos, transparencia y demás normas aplicables.

TÍTULO II

SISTEMA NACIONAL DE SEGURIDAD PENITENCIARIA TECNOLÓGICA E INTEGRAL

Artículo 7.- Creación funcional del Sistema. Se establece el Sistema Nacional de Seguridad Penitenciaria Tecnológica e Integral como marco de coordinación de las políticas, procesos, tecnologías, personas, información y controles destinados a proteger los establecimientos penitenciarios y correccionales.

Artículo 8.- Rectoría y coordinación. El Ministerio de Justicia ejercerá las funciones de dirección, coordinación y formulación de políticas que le correspondan conforme a la legislación vigente, en articulación con la Dirección General de Servicios Penitenciarios y Correccionales y las demás instituciones competentes.

Artículo 9.- Gestión operacional. La Dirección General de Servicios Penitenciarios y Correccionales ejecutará las medidas operativas que correspondan a sus atribuciones legales, incluyendo los controles institucionales de seguridad, acceso, custodia, movilidad, infraestructura y gestión de incidentes.

Artículo 10.- Coordinación interinstitucional. El sistema podrá articular, dentro de las competencias de cada institución, al Ministerio Público, Poder Judicial, Instituto Dominicano de las Telecomunicaciones, Policía Nacional, órganos de control, organismos de protección de datos y demás entidades públicas cuya participación resulte legalmente procedente.

Artículo 11.- Unidad técnica especializada. El Ministerio de Justicia dispondrá, conforme a su organización legal y reglamentaria, de una estructura especializada para coordinar los componentes tecnológicos de seguridad penitenciaria. Su organización, perfiles, procedimientos y relaciones internas serán definidos reglamentariamente.

Artículo 12.- Centro Nacional de Monitoreo. Se establecerá un centro técnico de monitoreo y análisis como mecanismo de apoyo a la supervisión nacional. No constituirá una autoridad paralela al Ministerio Público, al Poder Judicial ni a los órganos de investigación o seguridad, y actuará dentro de las competencias institucionales establecidas por la ley.

Artículo 13.- Responsabilidad institucional. Cada órgano participante será responsable de las funciones que legalmente le correspondan. La coordinación no podrá utilizarse para transferir, ampliar o asumir competencias que la Constitución o las leyes hayan atribuido a otra autoridad.

TÍTULO III

PREVENCIÓN, DETECCIÓN Y CONTROL DE DISPOSITIVOS DE COMUNICACIÓN NO AUTORIZADOS

Artículo 14.- Prevención del ingreso. Los establecimientos deberán implementar medidas proporcionales de prevención para impedir el ingreso de teléfonos celulares, dispositivos de comunicación, componentes tecnológicos y accesorios no autorizados, mediante controles de personas, vehículos, bienes, paquetes, herramientas, suministros y zonas de acceso.

Artículo 15.- Sistema de detección. Los establecimientos podrán utilizar tecnologías de detección y localización de dispositivos no autorizados, seleccionadas conforme a criterios de necesidad, eficacia, seguridad, interoperabilidad, protección de derechos, mantenimiento y costo total de propiedad.

Artículo 16.- Control técnico de comunicaciones. Las autoridades competentes podrán implementar mecanismos técnicos de control de comunicaciones dentro de los establecimientos penitenciarios únicamente cuando sean compatibles con la Constitución, la legislación vigente y las competencias de las autoridades reguladoras y judiciales correspondientes.

Artículo 17.- Prohibición de tecnologías destructivas. Queda prohibida la utilización deliberada de instalaciones eléctricas, equipos de energía, campos electromagnéticos u otros medios destinados a destruir, deteriorar o inutilizar físicamente dispositivos de comunicación cuando ello pueda comprometer la seguridad de las personas, las instalaciones o los servicios esenciales. La infraestructura eléctrica podrá utilizarse para fines legítimos de seguridad, continuidad, monitoreo y detección de anomalías.

Artículo 18.- Alertas y verificación humana. Las alertas generadas por sistemas tecnológicos deberán ser verificadas por personal autorizado antes de adoptar medidas que afecten derechos, imponer consecuencias administrativas o iniciar actuaciones disciplinarias, salvo las actuaciones urgentes de protección y seguridad permitidas por la ley.

Artículo 19.- Respuesta ante detección. La detección de un dispositivo no autorizado dará lugar, según su nivel de riesgo, a las actuaciones institucionales previstas en los protocolos de respuesta, incluyendo verificación, aislamiento preventivo cuando sea legalmente procedente, incautación o entrega a la autoridad competente, preservación de evidencia, documentación e investigación del origen del dispositivo.

Artículo 20.- Identificación técnica. Cuando resulte legalmente procedente, podrán registrarse identificadores técnicos del dispositivo, tarjeta o servicio asociado, sin que la

identificación técnica implique por sí misma autorización para acceder al contenido de comunicaciones o datos protegidos.

Artículo 21.- Intercepción y contenido. Ninguna disposición de esta ley se interpretará como autorización general para interceptar, grabar, escuchar, acceder o revelar el contenido de comunicaciones privadas. Tales actuaciones estarán sujetas al régimen constitucional, legal y judicial aplicable.

Artículo 22.- Prevención de puntos ciegos. Los sistemas de seguridad deberán identificar y corregir progresivamente zonas, procedimientos, horarios o actividades que presenten vulnerabilidades para el ingreso, ocultamiento, intercambio o utilización clandestina de dispositivos.

Artículo 23.- Pruebas de seguridad. La administración podrá realizar pruebas controladas de penetración física, tecnológica y procedimental, debidamente autorizadas y documentadas, para comprobar la eficacia de los controles. Las pruebas no podrán poner en riesgo innecesario a personas ni instalaciones.

Artículo 24.- Evaluación periódica. La eficacia de las medidas será evaluada mediante indicadores de prevención, detección, localización, respuesta, reincidencia, disponibilidad tecnológica, mantenimiento, incidentes internos y vulnerabilidades corregidas.

TÍTULO IV

COMUNICACIONES LEGÍTIMAS Y SERVICIOS TECNOLÓGICOS PARA PERSONAS PRIVADAS DE LIBERTAD

Artículo 25.- Comunicación legítima como componente de seguridad. El Estado promoverá mecanismos institucionales seguros y supervisados para satisfacer necesidades legítimas de comunicación de las personas privadas de libertad, sin perjuicio de las restricciones legalmente justificadas.

Artículo 26.- Servicios institucionales. Podrán habilitarse telefonía institucional, videocomunicación, comunicaciones legales y consulares, y otros servicios tecnológicos controlados, conforme a reglamento.

Artículo 27.- Acceso razonable. Los mecanismos de comunicación legítima procurarán condiciones razonables de acceso, horarios, identificación de usuarios y destinatarios, registro de uso y mecanismos de reclamación, de conformidad con la normativa aplicable.

Artículo 28.- Protección de comunicaciones privilegiadas. Las comunicaciones que gocen de protección constitucional o legal especial recibirán las garantías correspondientes. Los controles de seguridad no podrán convertirse en mecanismos de acceso indebido a información protegida.

Artículo 29.- Servicios digitales controlados. La administración podrá desarrollar servicios digitales educativos, administrativos, formativos o de reinserción en entornos controlados, con medidas de ciberseguridad y protección de datos.

Artículo 30.- Alfabetización digital. Los programas de formación podrán incorporar alfabetización digital, seguridad informática y uso responsable de herramientas tecnológicas.

TÍTULO V

INFORMACIÓN, INTELIGENCIA, MONITOREO Y EVIDENCIA DIGITAL

Artículo 31.- Sistema de información. El sistema penitenciario dispondrá de mecanismos integrados para registrar incidentes, alertas, controles, inventarios, accesos, mantenimientos y demás información necesaria para la seguridad, conforme a las normas de protección de datos.

Artículo 32.- Finalidad y minimización. La información será recopilada y tratada para finalidades legítimas, específicas y necesarias. Se limitará el acceso a la información al personal autorizado y según sus funciones.

Artículo 33.- Inteligencia penitenciaria. La información podrá utilizarse para análisis estratégico y operacional orientado a identificar riesgos, patrones de incidentes, vulnerabilidades, posibles redes de complicidad y tendencias, dentro del marco legal.

Artículo 34.- Evidencia digital. La obtención, preservación, documentación, traslado, análisis y presentación de evidencia digital se realizará conforme a las reglas constitucionales, procesales y técnicas aplicables.

Artículo 35.- Cadena de custodia. Los dispositivos y evidencias incautados deberán ser identificados, preservados, documentados y entregados a la autoridad competente mediante procedimientos que aseguren su integridad y trazabilidad.

Artículo 36.- Separación entre información e investigación penal. El análisis institucional de seguridad no sustituye las funciones de investigación y persecución penal del Ministerio Público ni las funciones jurisdiccionales del Poder Judicial.

Artículo 37.- Inteligencia artificial. Las herramientas de inteligencia artificial podrán utilizarse como apoyo para detección de anomalías, análisis de patrones, priorización de alertas, mantenimiento predictivo y gestión de riesgos, siempre bajo supervisión humana.

Artículo 38.- Límites a decisiones automatizadas. Ningún sistema automatizado podrá, por sí solo, determinar responsabilidad penal, imponer sanciones, ordenar registros invasivos, negar derechos o clasificar definitivamente a una persona como responsable de una conducta ilícita.

Artículo 39.- Auditoría de sistemas. Los sistemas automatizados utilizados para seguridad deberán mantener registros técnicos suficientes para permitir auditoría, revisión de resultados, identificación de errores y determinación de responsabilidades.

TÍTULO VI

CONTROL DE ACCESO, PERSONAS, VEHÍCULOS, BIENES E INFRAESTRUCTURA

Artículo 40.- Control de acceso. Todo establecimiento establecerá controles de identidad, autorización, ingreso, permanencia y salida de personas, vehículos, bienes, herramientas y equipos, diferenciados según el nivel de riesgo.

Artículo 41.- Trazabilidad. Los accesos y movimientos relevantes deberán quedar registrados mediante mecanismos proporcionales y seguros, permitiendo reconstruir eventos cuando sea necesario.

Artículo 42.- Personal, contratistas y proveedores. El personal y los terceros autorizados estarán sujetos a controles de identificación, autorización, capacitación y trazabilidad compatibles con sus funciones y derechos.

Artículo 43.- Visitantes. Las visitas serán sometidas a controles establecidos reglamentariamente, respetando las garantías especiales aplicables a abogados, representantes consulares, autoridades y otras personas con funciones legalmente protegidas.

Artículo 44.- Vehículos y bienes. Los vehículos, paquetes, herramientas, suministros, alimentos, medicamentos y componentes tecnológicos estarán sujetos a controles de ingreso, inventario y salida según su nivel de riesgo.

Artículo 45.- Zonas críticas. Los establecimientos identificarán zonas críticas y establecerán controles reforzados de acceso, acompañamiento, doble control o autorización especial cuando sea necesario.

Artículo 46.- Infraestructura crítica. La administración protegerá las instalaciones eléctricas, centros de datos, sistemas de comunicaciones, cámaras, controles de acceso, sistemas de respaldo, agua, climatización y demás infraestructura crítica.

Artículo 47.- Continuidad. Los sistemas esenciales deberán contar, de acuerdo con el nivel de riesgo y disponibilidad presupuestaria, con mecanismos de respaldo, recuperación y continuidad operacional.

TÍTULO VII

PERSONAL, CAPACITACIÓN, INTEGRIDAD Y PREVENCIÓN DE CORRUPCIÓN

Artículo 48.- Capacitación. El personal que desempeñe funciones críticas de seguridad deberá recibir capacitación inicial, especializada y continua, conforme a perfiles de competencia.

Artículo 49.- Certificación. Las funciones técnicas o críticas que determine el reglamento podrán requerir certificación y recertificación periódica.

Artículo 50.- Integridad institucional. La administración adoptará medidas para prevenir conflictos de interés, corrupción, complicidad, manipulación de controles y utilización indebida de sistemas.

Artículo 51.- Separación de funciones. Cuando el nivel de riesgo lo justifique, las funciones de autorización, operación, supervisión, auditoría y administración tecnológica serán distribuidas de manera que se reduzcan oportunidades de abuso.

Artículo 52.- Rotación y controles. La rotación funcional podrá utilizarse como mecanismo preventivo cuando resulte necesaria y compatible con la continuidad, profesionalización y derechos del personal.

Artículo 53.- Denuncia y protección. Se establecerán canales seguros para reportar irregularidades y medidas de protección frente a represalias, de conformidad con el ordenamiento aplicable.

Artículo 54.- Responsabilidad del personal. La responsabilidad administrativa, disciplinaria, civil o penal se determinará conforme a las normas vigentes, atendiendo a la naturaleza de la conducta, el daño, la intención y las circunstancias.

TÍTULO VIII

RESPUESTA A INCIDENTES, INVESTIGACIÓN Y COORDINACIÓN INTERINSTITUCIONAL

Artículo 55.- Gestión integral de incidentes. Los incidentes seguirán un ciclo de alerta, validación, control, preservación, intervención, documentación, investigación, decisión, corrección y cierre.

Artículo 56.- Clasificación de incidentes. El reglamento establecerá categorías de severidad y criterios para activar respuestas proporcionales.

Artículo 57.- Protección inmediata. La prioridad inicial será proteger la vida, integridad y seguridad de las personas y evitar la continuidad del riesgo.

Artículo 58.- Preservación de evidencia. Cuando exista posible relevancia penal o disciplinaria, deberán preservarse registros, imágenes, dispositivos, accesos y demás evidencias conforme a la normativa aplicable.

Artículo 59.- Coordinación con el Ministerio Público. Cuando los hechos puedan constituir infracción penal, se dará intervención al Ministerio Público conforme a sus competencias legales.

Artículo 60.- Investigación de origen. Los incidentes relevantes serán analizados para determinar, cuando sea posible, cómo ocurrió el ingreso o utilización del dispositivo, qué controles fallaron y qué medidas deben corregirse.

Artículo 61.- Revisión posterior. Los incidentes graves deberán generar una revisión posterior orientada a identificar causas raíz, responsabilidades y medidas correctivas, sin sustituir las investigaciones legales correspondientes.

TÍTULO IX

CIBERSEGURIDAD, PROTECCIÓN DE DATOS Y CONTINUIDAD OPERACIONAL

Artículo 62.- Seguridad por diseño. Los sistemas tecnológicos penitenciarios deberán incorporar medidas de seguridad desde su diseño, adquisición, implementación, operación y retiro.

Artículo 63.- Gestión de identidades. El acceso a sistemas deberá basarse en identidades individuales, privilegios según funciones y mecanismos reforzados de autenticación cuando corresponda.

Artículo 64.- Registro y auditoría. Los accesos y operaciones relevantes deberán generar registros que permitan detectar usos indebidos y realizar auditorías.

Artículo 65.- Protección de datos personales. El tratamiento de datos personales se sujetará a la legislación vigente, incluyendo principios de finalidad, proporcionalidad, seguridad, confidencialidad, calidad y derechos de los titulares cuando sean aplicables.

Artículo 66.- Intercambio de información. El intercambio de información entre instituciones deberá contar con base jurídica, finalidad definida, controles de acceso, trazabilidad y medidas de seguridad.

Artículo 67.- Ciberincidentes. Los incidentes de ciberseguridad deberán gestionarse mediante procedimientos de detección, contención, recuperación, documentación y aprendizaje institucional.

Artículo 68.- Continuidad y recuperación. Los sistemas críticos deberán contar con mecanismos de respaldo, recuperación y continuidad adecuados al nivel de riesgo.

Artículo 69.- Acceso de proveedores. El acceso remoto de proveedores a sistemas penitenciarios deberá ser excepcional, controlado, limitado en el tiempo, registrado y sujeto a autorización.

TÍTULO X

TECNOLOGÍA, CONTRATACIÓN, EVALUACIÓN Y SOSTENIBILIDAD

Artículo 70.- Necesidad y evaluación previa. Toda adquisición tecnológica deberá responder a una necesidad documentada, evaluación de riesgos, análisis de alternativas, costo total de propiedad y compatibilidad con la arquitectura institucional.

Artículo 71.- Contratación pública. Las adquisiciones, obras y servicios derivados de esta ley se realizarán conforme al régimen vigente de contrataciones públicas, incluyendo la Ley núm. 47-25, su reglamento y las disposiciones que los sustituyan o complementen.

Artículo 72.- Homologación. Los sistemas críticos podrán estar sujetos a procesos de evaluación, pruebas y homologación antes de su despliegue nacional.

Artículo 73.- Interoperabilidad. Las tecnologías deberán favorecer la interoperabilidad, portabilidad de datos, documentación técnica y reducción de dependencias innecesarias de un único proveedor.

Artículo 74.- Pruebas de aceptación. La puesta en operación de soluciones críticas estará condicionada a pruebas de aceptación que acrediten funcionamiento, seguridad, rendimiento, disponibilidad y cumplimiento contractual.

Artículo 75.- Mantenimiento y ciclo de vida. Los contratos deberán contemplar mantenimiento, actualizaciones, soporte, capacitación, sustitución y retiro seguro cuando corresponda.

Artículo 76.- Evaluación independiente. Las tecnologías de mayor impacto en derechos, seguridad o continuidad podrán someterse a auditorías o evaluaciones independientes.

Artículo 77.- Prohibición de dependencia tecnológica injustificada. La administración procurará evitar dependencias que impidan migrar, mantener, auditar o sustituir sistemas críticos cuando existan alternativas razonables.

Artículo 78.- Sostenibilidad financiera. La planificación presupuestaria deberá considerar adquisición, instalación, licenciamiento, conectividad, mantenimiento, capacitación, reposición y retiro durante el ciclo de vida.

TÍTULO XI

RESPONSABILIDADES, INFRACCIONES Y REMISIÓN AL ORDENAMIENTO PENAL

Artículo 79.- Principio de legalidad sancionadora. Ninguna persona será sancionada por una conducta que no esté previamente tipificada como infracción administrativa, disciplinaria o penal por una norma con rango suficiente.

Artículo 80.- Conductas relacionadas con dispositivos no autorizados. La introducción, suministro, ocultamiento, posesión, facilitación, utilización, manipulación o extracción de dispositivos no autorizados podrá generar las consecuencias jurídicas previstas en el ordenamiento, según la condición del responsable y la naturaleza de la conducta.

Artículo 81.- Remisión al Código Penal. Cuando una conducta constituya delito, su investigación, calificación y sanción se regirán por el Código Penal vigente y las normas procesales aplicables. La presente ley no crea por sí misma nuevos delitos ni penas mediante reglamento.

Artículo 82.- Responsabilidad administrativa y disciplinaria. Las conductas que constituyan faltas administrativas o disciplinarias serán conocidas conforme al régimen jurídico aplicable al servidor público, contratista, proveedor o tercero responsable.

Artículo 83.- Agravación por función o posición. Cuando la legislación aplicable contemple agravaciones por abuso de función, autoridad, custodia, confianza o participación organizada, estas serán aplicadas por la autoridad competente conforme al ordenamiento vigente.

Artículo 84.- Debido proceso. Toda actuación sancionadora deberá respetar competencia, notificación, defensa, prueba, motivación, proporcionalidad, impugnación y demás garantías aplicables.

Artículo 85.- No responsabilidad automática. La generación de una alerta tecnológica, por sí sola, no constituirá prueba concluyente de responsabilidad penal o disciplinaria.

TÍTULO XII

TRANSPARENCIA, EVALUACIÓN, TRANSITORIAS Y FINALES

Artículo 86.- Indicadores nacionales. El Ministerio de Justicia establecerá indicadores de prevención, detección, respuesta, investigación, integridad, disponibilidad tecnológica, mantenimiento, capacitación, costos y resultados.

Artículo 87.- Evaluación periódica. El sistema será evaluado periódicamente mediante auditorías, pruebas, indicadores, revisiones de incidentes y evaluaciones externas cuando corresponda.

Artículo 88.- Información pública. Se publicará información agregada sobre avances, inversiones, resultados e indicadores, preservando la información cuya reserva sea necesaria conforme a la Constitución y las leyes.

Artículo 89.- Plan nacional de implementación. La administración elaborará un plan nacional de implementación con diagnóstico, priorización por riesgo, pilotos, evaluación, expansión, capacitación, mantenimiento y sostenibilidad.

Artículo 90.- Fases de implementación. La implementación podrá desarrollarse progresivamente en fases de diagnóstico y contención inicial, pilotos, evaluación, expansión priorizada, cobertura nacional y consolidación.

Artículo 91.- Continuidad de contratos y sistemas existentes. Los sistemas y contratos existentes serán evaluados y armonizados progresivamente con esta ley, respetando los derechos adquiridos y las reglas aplicables a los procedimientos de contratación en curso.

Artículo 92.- Reglamento. El Poder Ejecutivo dictará las disposiciones reglamentarias necesarias para la aplicación de esta ley, dentro del ámbito de sus competencias.

Artículo 93.- Protocolos y manuales técnicos. Los aspectos operativos, técnicos, de mantenimiento, pruebas, interoperabilidad, respuesta a incidentes y certificación serán desarrollados mediante protocolos y manuales institucionales compatibles con esta ley y su reglamento.

Artículo 94.- Revisión periódica. El marco nacional será revisado periódicamente para incorporar cambios tecnológicos, jurisprudenciales, legislativos y operacionales.

Artículo 95.- Armonización normativa. Las disposiciones reglamentarias, administrativas y contractuales deberán armonizarse con la presente ley y con el ordenamiento jurídico vigente.

Artículo 96.- Derogaciones. Quedan derogadas las disposiciones de igual o inferior rango que sean contrarias a la presente ley, sin perjuicio de los regímenes especiales y normas superiores que resulten aplicables.

Artículo 97.- Entrada en vigor. La presente ley entrará en vigor conforme a las reglas constitucionales y legales aplicables.

Artículo 98.- Disposición de cierre. La aplicación de esta ley tendrá como finalidad fortalecer simultáneamente la seguridad penitenciaria, la protección de las personas, la integridad institucional, la reinserción y la capacidad del Estado para prevenir, detectar, investigar y corregir riesgos asociados al uso clandestino de tecnologías.