PROPUESTA DE POLÍTICA PÚBLICA
SISTEMA NACIONAL DE SEGURIDAD PENITENCIARIA INTEGRAL, TECNOLOGICA Y DE COMUNICACIONES

Documento Marco

RD Propone RD Propone

CAPÍTULO I
FUNDAMENTACIÓN, DIAGNÓSTICO Y PROPÓSITO GENERAL

1. Introducción

La seguridad penitenciaria constituye un componente esencial de la seguridad ciudadana. La privación de libertad dispuesta por una autoridad judicial no puede limitarse al confinamiento físico de una persona dentro de un establecimiento penitenciario; debe garantizar igualmente que dicho establecimiento no pueda ser utilizado como plataforma para continuar, organizar, facilitar o dirigir actividades delictivas hacia el exterior.

La utilización clandestina de teléfonos celulares, tarjetas SIM, dispositivos de comunicación, acceso a internet y otros medios tecnológicos dentro de los centros penitenciarios representa, por tanto, un riesgo que trasciende el orden interno de las cárceles. Cuando una persona privada de libertad consigue mantener comunicaciones no autorizadas con el exterior, puede conservar capacidad operativa para coordinar actividades criminales, contactar integrantes de organizaciones delictivas, intimidar víctimas o testigos, realizar fraudes, extorsiones u otras acciones contrarias a la ley.

La respuesta del Estado frente a esta problemática no debe descansar exclusivamente sobre la instalación de equipos bloqueadores de señales. Aunque estos constituyen una herramienta importante y la República Dominicana ya ha iniciado proyectos dirigidos a su utilización en centros penitenciarios, la naturaleza cambiante de las tecnologías de comunicación, las posibilidades de evasión y, especialmente, los mecanismos mediante los cuales los dispositivos ingresan y permanecen operativos dentro de los establecimientos exigen una política pública integral.

La presente propuesta plantea la creación de un *Sistema Nacional para la Prevención y Neutralización de Comunicaciones Ilícitas en Centros Penitenciarios*, sustentado en un modelo de seguridad por capas que actúe simultáneamente sobre el ingreso de dispositivos, su ocultamiento, alimentación eléctrica, acceso a redes de telecomunicaciones, utilización, detección, decomiso, trazabilidad y las responsabilidades derivadas de su introducción o facilitación.

La finalidad no será impedir las comunicaciones legítimas de las personas privadas de libertad con sus familiares, defensores, autoridades u otras personas autorizadas. Por el contrario, la política deberá desarrollar canales institucionales seguros, controlados y

RD Propone RD Propone

compatibles con los derechos fundamentales, diferenciando claramente entre la comunicación legítima y aquella realizada mediante dispositivos clandestinos.

2. Planteamiento del problema

La introducción de teléfonos celulares y otros dispositivos electrónicos dentro de los establecimientos penitenciarios constituye una vulnerabilidad estructural cuando los mecanismos tradicionales de inspección permiten que dichos equipos puedan atravesar los controles de acceso.

El problema debe analizarse como una cadena. Para que un celular clandestino pueda utilizarse dentro de una prisión deben producirse, generalmente, varias condiciones sucesivas:

a) El dispositivo debe ingresar al establecimiento;

b) Debe superar los controles físicos y tecnológicos existentes;

c) Debe ser entregado u ocultado dentro del recinto;

d) Debe disponer de una tarjeta SIM, conexión celular, acceso inalámbrico u otra forma de comunicación;

e) Debe disponer de energía suficiente para mantenerse operativo;

f) Su utilización debe evitar ser detectada por el personal o por los sistemas tecnológicos;

g) Debe existir alguna posibilidad de conservarlo, esconderlo, trasladarlo o reemplazarlo.

Esta cadena demuestra que la neutralización efectiva del problema no depende de una única medida. Si el Estado concentra toda su estrategia en bloquear la señal, pero permite que los dispositivos continúen entrando, permanecerá constantemente intentando neutralizar equipos clandestinos ya introducidos.

Si únicamente fortalece las requisas, pero permite que los teléfonos que logren superar los controles tengan señal, energía y lugares donde esconderse, permanecerá abierta otra vulnerabilidad. En consecuencia, la estrategia propuesta parte de un principio fundamental:

Cada dispositivo clandestino deberá enfrentar múltiples barreras independientes y acumulativas, de manera que superar una de ellas no permita automáticamente su utilización.

3. Cambio de paradigma

RD Propone RD Propone

La política pública propuesta sustituye el enfoque de una sola barrera por un modelo denominado *Defensa Penitenciaria por Capas.*

El objetivo consiste en conseguir que para utilizar clandestinamente un dispositivo dentro de un establecimiento penitenciario sea necesario superar sucesivamente controles físicos, humanos, tecnológicos, eléctricos, radioeléctricos, administrativos y disciplinarios. Bajo este modelo, un teléfono ilegal tendría que:

Entrar sin ser detectado / Ser ocultado / Conseguir energía / Conseguir acceso a una red / Evitar los sistemas de detección / Utilizarse sin generar alertas / Evitar su localización / Evitar su decomiso / Evitar la identificación de la persona que lo introdujo o facilitó.

Mientras mayor sea el número de obstáculos independientes, menor será la posibilidad de utilización sostenida del dispositivo.

La política no perseguirá técnicamente destruir teléfonos mediante instalaciones eléctricas u otros mecanismos que puedan generar riesgos para las personas, incendios, electrocución o daños sobre equipos legítimos. En cambio, se procurará que las áreas destinadas a personas privadas de libertad cuenten con instalaciones eléctricas diseñadas de forma que dificulten o impidan la conexión clandestina de cargadores y dispositivos no autorizados, conforme a normas de ingeniería y seguridad.

4. Anillos de seguridad

El sistema se estructurará inicialmente alrededor de seis grandes anillos.

Primer anillo: Prevención del ingreso

Su propósito será impedir que teléfonos, tarjetas SIM, cargadores, baterías externas, cables, adaptadores, dispositivos de almacenamiento y otros componentes tecnológicos ingresen clandestinamente a los centros penitenciarios.

Los controles alcanzarán a visitantes, funcionarios, agentes penitenciarios, contratistas, suplidores, profesionales, vehículos, correspondencia, paquetes, alimentos, mercancías y cualquier otro canal de acceso.

El principio rector será que ninguna categoría de persona quede automáticamente exenta de controles por razón de su función.

Segundo anillo: Detección y trazabilidad interna

RD Propone RD Propone

Partiendo de que ningún sistema de entrada puede considerarse absolutamente infalible, los establecimientos deberán disponer de mecanismos para localizar equipos que hayan conseguido atravesar el primer anillo.

Esto comprenderá videovigilancia, controles internos, detección de dispositivos electrónicos, inspecciones basadas en riesgo, registros tecnológicos y sistemas que permitan identificar áreas recurrentemente vinculadas con decomisos.

Cada dispositivo encontrado deberá convertirse además en fuente de inteligencia penitenciaria.

Su IMEI, SIM, características, lugar de hallazgo, fecha, hora y demás información técnicamente obtenible conforme a la ley deberán registrarse para detectar patrones, reincidencias y posibles redes de introducción o distribución.

Tercer anillo: Neutralización de las comunicaciones

Los dispositivos clandestinos que logren ingresar no deberán disponer libremente de acceso a las redes públicas de telecomunicaciones.

Para tales fines se desarrollará, conjuntamente con INDOTEL y las prestadoras de servicios de telecomunicaciones, una arquitectura que podrá combinar tecnologías de bloqueo técnicamente autorizadas, sistemas de acceso administrado, identificación de terminales, listas de dispositivos permitidos y otras soluciones compatibles con el régimen dominicano de telecomunicaciones.

Las medidas deberán diseñarse de manera que su efecto quede limitado al perímetro penitenciario correspondiente y no afecte injustificadamente las comunicaciones legítimas de comunidades, viviendas, empresas o servicios de emergencia situados en áreas circundantes.

Cuarto anillo: Control de alimentación eléctrica

La energía constituye una vulnerabilidad frecuentemente ignorada en la seguridad penitenciaria. Un teléfono clandestino necesita ser cargado repetidamente para conservar su utilidad.

Por esta razón, los nuevos centros penitenciarios y las remodelaciones progresivas de los existentes deberán incorporar criterios de *seguridad eléctrica penitenciaria*.

RD Propone RD Propone

Las áreas de alojamiento de internos deberán reducir al mínimo necesario los tomacorrientes convencionales de libre acceso.

Los circuitos destinados a iluminación, ventilación y otros servicios esenciales podrán diseñarse de manera separada de aquellos destinados a equipos conectables.

Cuando resulte necesario disponer de puntos de alimentación eléctrica, podrán incorporarse mecanismos de protección contra manipulación, temporización, control de acceso, medición de consumo y otras tecnologías que permitan detectar usos no autorizados.

En ningún caso se utilizarán mecanismos destinados deliberadamente a provocar descargas, sobretensiones u otras condiciones capaces de dañar clandestinamente dispositivos conectados, debido a los riesgos para la integridad física, la seguridad contra incendios y los equipos legítimos.

El objetivo será *impedir o dificultar la carga*, no destruir eléctricamente el dispositivo.

Quinto anillo: Responsabilidad y consecuencias

La introducción de dispositivos prohibidos deberá generar consecuencias proporcionales a la condición de la persona responsable y a la finalidad de la conducta. La política diferenciará claramente entre:

a) La posesión o utilización por una persona privada de libertad;

b) La introducción deliberada por visitantes;

c) La participación de contratistas o suplidores;

d) La facilitación, tolerancia o introducción deliberada realizada por funcionarios o agentes del sistema penitenciario;

e) La introducción asociada a organizaciones criminales o destinada a facilitar otros delitos.

Se evaluará el régimen vigente para determinar dónde existen sanciones suficientes y dónde resulta necesaria una modificación legislativa.

La intervención de un funcionario encargado de la custodia deberá recibir particular atención, debido al deber especial asociado a su posición y al daño institucional que produce la utilización de sus funciones para facilitar contrabando penitenciario.

RD Propone RD Propone

Toda modificación sancionadora deberá respetar los principios constitucionales de legalidad, proporcionalidad, debido proceso, presunción de inocencia y derecho de defensa.

Sexto anillo: Integridad institucional y lucha contra la complicidad interna

La política reconocerá expresamente que el problema de los celulares clandestinos no puede abordarse únicamente desde la conducta de las personas privadas de libertad.

Deberán identificarse y reducirse las oportunidades de corrupción, complicidad, negligencia o participación del personal que tenga acceso a los establecimientos penitenciarios.

Para ello se establecerán controles diferenciados para funcionarios, rotación razonable en posiciones particularmente sensibles, trazabilidad de accesos, cámaras en puntos críticos, auditorías, controles de inventario, mecanismos confidenciales de denuncia y análisis sistemático de patrones de decomisos.

Cuando exista evidencia de participación de servidores públicos, los casos deberán ser puestos a disposición de las autoridades competentes, sin perjuicio de las medidas disciplinarias correspondientes.

5. Objetivo general

Crear e implementar un sistema nacional permanente destinado a prevenir, detectar, neutralizar y reducir progresivamente la utilización de dispositivos de comunicación no autorizados dentro de los centros penitenciarios de la República Dominicana, mediante la integración coordinada de controles físicos, tecnológicos, eléctricos, administrativos, disciplinarios y de telecomunicaciones.

6. Objetivos específicos

La política tendrá como objetivos específicos:

a) Reducir sustancialmente la introducción clandestina de teléfonos y dispositivos electrónicos;

b) Detectar tempranamente los equipos que logren superar los controles de acceso;

c) Impedir o dificultar técnicamente su utilización dentro de los establecimientos;

d) Reducir las posibilidades de mantenerlos cargados y operativos;

RD Propone RD Propone

e) Identificar patrones de introducción, distribución y utilización;

f) Fortalecer la investigación de redes internas y externas relacionadas con el contrabando penitenciario;

g) Establecer responsabilidades claras para internos, visitantes, funcionarios, contratistas y terceros;

h) Proteger las comunicaciones legales y autorizadas de las personas privadas de libertad;

i) Evitar afectaciones indebidas a las telecomunicaciones de las comunidades próximas a los establecimientos;

j) Crear mecanismos permanentes de auditoría y evaluación de resultados.

7. Principios rectores

La implementación del sistema estará guiada por los principios de legalidad, dignidad humana, seguridad pública, proporcionalidad, prevención, responsabilidad, trazabilidad, integridad institucional, protección de derechos fundamentales, neutralidad tecnológica, coordinación interinstitucional, evaluación permanente y mejora continua.

La seguridad penitenciaria deberá ser compatible con la función constitucional y legal de rehabilitación y reinserción social.

Las medidas tecnológicas no podrán utilizarse como mecanismos arbitrarios de aislamiento ni como sustitutos de las comunicaciones familiares, jurídicas o institucionales autorizadas.

8. Marco institucional preliminar

La dirección estratégica de la política corresponderá al *Ministerio de Justicia*, dentro de sus atribuciones relacionadas con la coordinación y supervisión del sistema penitenciario.

La ejecución operativa deberá articularse con la *Dirección General de Servicios Penitenciarios y Correccionales.*

El *Instituto Dominicano de las Telecomunicaciones (INDOTEL)* tendrá participación esencial en los componentes relacionados con espectro radioeléctrico, redes de telecomunicaciones, soluciones de bloqueo, acceso administrado y coordinación con las empresas prestadoras.

RD Propone RD Propone

Asimismo, deberán intervenir, según sus competencias, el Ministerio Público cuando existan indicios de hechos delictivos, las agencias de investigación correspondientes, organismos responsables de ciberseguridad y las prestadoras de servicios públicos de telecomunicaciones.

La política deberá apoyarse principalmente en la Ley núm. 113-21 sobre el Sistema Penitenciario y Correccional, la Ley núm. 80-25 Orgánica del Ministerio de Justicia, la Ley núm. 153-98 General de Telecomunicaciones, la Constitución de la República y demás disposiciones legales y reglamentarias aplicables.

9. Propósito final

El propósito de esta política no será declarar imposible la existencia de un teléfono clandestino dentro de una prisión, objetivo que difícilmente puede garantizarse de forma absoluta. Su propósito será mucho más operativo y verificable:

Hacer extraordinariamente difícil introducirlo, ocultarlo, cargarlo, conectarlo, utilizarlo y conservarlo sin ser detectado, y elevar significativamente la probabilidad de identificar a las personas que participen en su introducción o utilización ilícita.

La efectividad del sistema no se medirá por la cantidad de equipos instalados ni por el número de operativos realizados, sino por resultados verificables tales como la reducción de teléfonos decomisados, disminución de conexiones clandestinas detectadas, reducción de reincidencias, identificación de redes de introducción, eliminación de zonas de cobertura irregular y disminución de delitos coordinados desde establecimientos penitenciarios.

CAPÍTULO II
SISTEMA DE PREVENCIÓN DEL INGRESO DE DISPOSITIVOS Y COMPONENTES PROHIBIDOS

1. Objeto del capítulo

El presente capítulo establece los lineamientos para prevenir la introducción clandestina de teléfonos celulares, tarjetas SIM, cargadores, baterías portátiles, cables, adaptadores, dispositivos de almacenamiento, equipos de comunicación inalámbrica y otros componentes tecnológicos no autorizados dentro de los centros penitenciarios de la República Dominicana.

RD Propone RD Propone

La política parte del principio de que la primera y más eficiente medida de neutralización consiste en evitar que el dispositivo alcance las áreas donde permanecen las personas privadas de libertad.

La prevención del ingreso deberá operar mediante controles diferenciados pero igualmente rigurosos sobre visitantes, funcionarios, agentes penitenciarios, contratistas, proveedores, profesionales, vehículos, mercancías, correspondencia y cualquier otra persona u objeto que acceda al recinto.

2. Principio de control universal

Ninguna persona que ingrese a un establecimiento penitenciario estará automáticamente excluida de los procedimientos de seguridad por razón de su cargo, profesión, relación institucional o frecuencia de acceso.

Los protocolos deberán distinguir los niveles de revisión según el riesgo, pero deberán procurar que todo ingreso pueda ser objeto de verificación.

El personal penitenciario, contratistas y proveedores estarán sujetos a controles específicos debido a la frecuencia y naturaleza de su acceso.

Las excepciones necesarias por razones operativas deberán quedar expresamente documentadas y ser auditables.

3. Clasificación de objetos tecnológicos prohibidos

El sistema penitenciario establecerá y actualizará periódicamente un catálogo nacional de objetos tecnológicos cuyo ingreso, posesión o utilización requiera autorización. Entre ellos se incluirán:

a) Teléfonos celulares;

b) Tarjetas SIM físicas y otros elementos equivalentes de identificación móvil;

c) Relojes inteligentes y dispositivos con capacidad de comunicación;

d) Módems, routers y equipos portátiles de conectividad;

e) Baterías externas o bancos de energía;

f) Cargadores eléctricos;

g) Cables USB o equivalentes;

RD Propone RD Propone

h) Adaptadores eléctricos;

i) Auriculares con capacidad de comunicación o almacenamiento;

j) Dispositivos de almacenamiento digital;

k) Componentes electrónicos que puedan utilizarse para ensamblar o alimentar equipos de comunicación;

l) Cualquier nueva tecnología que permita establecer comunicaciones no autorizadas.

La clasificación deberá actualizarse conforme evolucione la tecnología.

4. Registro Nacional de Dispositivos Autorizados

Se creará un Registro Nacional de Dispositivos Tecnológicos Autorizados para Centros Penitenciarios. Todo equipo autorizado para ingresar deberá estar asociado, cuando técnicamente resulte posible, a:

a) Persona responsable;

b) Institución;

c) Número telefónico;

d) Número IMEI;

e) Identificación de la tarjeta SIM;

f) Marca y modelo;

g) Número de serie;

h) Centro donde podrá utilizarse;

i) Área autorizada;

j) Período de autorización.

Cada autorización deberá tener fecha de inicio y vencimiento.

Los dispositivos institucionales deberán identificarse físicamente mediante elementos resistentes a manipulación y, cuando sea posible, mediante identificación electrónica.

5. Política de teléfonos personales del personal

RD Propone RD Propone

Como regla general, los teléfonos celulares personales del personal penitenciario no deberán ingresar a las áreas de internamiento. Los centros deberán disponer de casilleros seguros situados antes de la zona restringida.

El funcionario depositará su dispositivo personal antes de ingresar y podrá recuperarlo al finalizar su jornada o cuando abandone temporalmente el área controlada.

Las funciones que requieran comunicación móvil institucional deberán utilizar dispositivos oficiales previamente registrados. El objetivo será eliminar la práctica de utilizar teléfonos particulares dentro de las áreas sensibles.

6. Control de visitantes

Toda persona visitante deberá atravesar un proceso estandarizado de control antes de acceder a las áreas de visitas. El proceso podrá comprender:

a) Verificación de identidad;

b) Confirmación de autorización de visita;

c) Registro electrónico de entrada;

d) Depósito obligatorio de dispositivos electrónicos no autorizados;

e) Inspección mediante detectores de metales;

f) Revisión de objetos personales;

g) Inspección adicional cuando existan indicadores objetivos de riesgo.

El diseño de los controles deberá respetar la dignidad, privacidad y derechos fundamentales de los visitantes. Los procedimientos más intrusivos deberán estar sometidos a reglas claras, supervisión y garantías legales.

7. Tecnologías de inspección

Los establecimientos podrán incorporar progresivamente tecnologías diseñadas para detectar objetos ocultos. Estas podrán incluir, conforme a las características de cada centro:

- Detectores de metales de arco.
- Detectores manuales.
- Sistemas de inspección mediante rayos X para equipajes y paquetes.
- Equipos especializados para detectar componentes electrónicos.

RD Propone RD Propone

- Sistemas de inspección corporal técnicamente apropiados cuando su utilización se encuentre legalmente habilitada.

La tecnología nunca sustituirá completamente al personal de seguridad, sino que deberá funcionar como herramienta de apoyo.

8. Segundo nivel de inspección

Cuando un primer control produzca una alerta, el sistema deberá disponer de un procedimiento de inspección secundaria. Esta deberá realizarse en un área especialmente acondicionada, bajo videovigilancia cuando resulte legalmente admisible y respetando la privacidad de la persona. Cada inspección secundaria deberá registrar:

- Fecha.
- Hora.
- Persona.
- Motivo de la alerta.
- Resultado.
- Funcionario responsable.
- Objetos encontrados.

Las estadísticas deberán permitir identificar patrones de intentos de introducción.

9. Control del personal penitenciario

La política establecerá controles de entrada y salida aplicables al personal según criterios objetivos de riesgo. Podrán incluirse inspecciones aleatorias, controles electrónicos y verificación de pertenencias.

La selección aleatoria deberá realizarse mediante mecanismos que reduzcan la posibilidad de manipulación por supervisores o funcionarios. Los procedimientos no deberán utilizarse como mecanismos de persecución laboral ni discriminación.

10. Control de contratistas y suplidores

Los contratistas, trabajadores temporales, técnicos de mantenimiento, suplidores y personal de empresas externas estarán sometidos a controles equivalentes a los establecidos para otros ingresos.

Todo contratista deberá identificarse antes de acceder al establecimiento.

RD Propone RD Propone

Las herramientas y equipos tecnológicos deberán inventariarse al momento de entrada y verificarse nuevamente al salir. Cuando sea necesario introducir teléfonos, tablets, laptops u otros dispositivos por razones técnicas, deberán registrarse previamente.

El sistema deberá confirmar que el mismo equipo autorizado que ingresó sea el que posteriormente abandone el establecimiento.

11. Control de mercancías

Los alimentos, medicamentos, productos de higiene, ropa, materiales de construcción y demás mercancías destinadas al centro deberán ingresar exclusivamente por puntos oficialmente designados. Toda entrega deberá estar asociada a:

- Proveedor.
- Vehículo.
- Conductor.
- Fecha.
- Hora.
- Orden de entrega.
- Funcionario receptor.
- Área de destino.

Los paquetes deberán someterse a inspección física o tecnológica de acuerdo con su naturaleza. La recepción de mercancías fuera de los puntos establecidos deberá quedar prohibida salvo emergencia debidamente documentada.

12. Control de vehículos

Los vehículos autorizados para ingresar al perímetro interno deberán registrarse electrónicamente. El protocolo deberá permitir verificar tanto el vehículo como su carga.

Las zonas de carga y descarga deberán encontrarse bajo cobertura permanente de cámaras. Siempre que resulte operativamente posible, las mercancías deberán transferirse en áreas intermedias para reducir la necesidad de que vehículos externos accedan profundamente al recinto.

13. Áreas de transferencia segura

Los nuevos establecimientos penitenciarios y aquellos sometidos a remodelación deberán incorporar áreas de transferencia entre el exterior y el interior. Estas áreas funcionarán

RD Propone RD Propone

como una barrera física donde mercancías, herramientas o materiales puedan inspeccionarse antes de ingresar.

El diseño deberá impedir que una persona pueda pasar directamente desde el exterior hasta una zona penitenciaria sin atravesar los controles establecidos.

14. Videovigilancia de puntos de ingreso

Los principales puntos de acceso deberán contar con videovigilancia permanente. Las cámaras deberán cubrir:

- Entradas principales.
- Entradas del personal.
- Áreas de recepción de mercancías.
- Estacionamientos sensibles.
- Muelles de carga.
- Pasillos de transferencia.
- Zonas de inspección de objetos.
- Accesos vehiculares.

Las grabaciones deberán conservarse durante un período determinado conforme al marco jurídico aplicable y a reglas de protección de datos.

15. Trazabilidad de entrada y salida

Toda persona que acceda a un establecimiento deberá generar un registro verificable de entrada y salida. Este podrá incluir:

- Identidad.
- Categoría de acceso.
- Hora de entrada.
- Hora de salida.
- Áreas autorizadas.
- Funcionario o unidad responsable.

Cuando corresponda, dispositivos tecnológicos autorizados.

El sistema deberá permitir reconstruir posteriormente quién estuvo dentro del establecimiento durante un determinado período.

16. Control de áreas de alto riesgo

RD Propone RD Propone

Los centros deberán identificar mediante análisis periódico aquellas áreas donde históricamente se hayan producido decomisos o incidentes. Estas podrán recibir controles adicionales.

Las medidas deberán fundamentarse en datos y no únicamente en apreciaciones subjetivas. El mapa de riesgo deberá actualizarse periódicamente.

17. Prevención mediante análisis de patrones

Todos los intentos de introducción deberán convertirse en información útil. El sistema deberá analizar variables como:

- Tipo de objeto.
- Método utilizado para ocultarlo.
- Punto de entrada.
- Hora.
- Día.
- Persona involucrada.
- Funcionario que prestaba servicio.
- Empresa o proveedor relacionado.
- Centro penitenciario.

La acumulación de estos datos deberá permitir identificar nuevas modalidades y adaptar los controles.

18. Control de encomiendas y correspondencia

Todo paquete destinado a una persona privada de libertad deberá ser recibido mediante canales institucionales. No deberá permitirse la entrega directa fuera de los procedimientos autorizados.

Los paquetes podrán someterse a inspección mediante equipos tecnológicos o revisión física conforme al contenido. Cuando se detecten objetos prohibidos deberá preservarse la evidencia correspondiente cuando existan indicios de infracción penal.

19. Control sobre drones y lanzamiento desde el exterior

La política deberá reconocer expresamente el riesgo derivado del lanzamiento de objetos sobre muros o de la utilización de aeronaves no tripuladas. Cada centro realizará un análisis de su perímetro para determinar vulnerabilidades. Podrán adoptarse medidas como:

RD Propone RD Propone

- Videovigilancia perimetral.
- Iluminación exterior.
- Detección de movimientos.
- Protecciones físicas superiores en áreas especialmente vulnerables.
- Protocolos de respuesta frente a drones.
- Coordinación con autoridades competentes cuando se detecte actividad aérea sospechosa.

Las medidas de interferencia radioeléctrica contra aeronaves no tripuladas solo podrán utilizarse cuando sean legal y técnicamente autorizadas.

20. Diseño físico orientado a la prevención

La seguridad tecnológica deberá complementarse con arquitectura penitenciaria. Los centros deberán procurar:

- Reducir puntos ciegos.
- Separar adecuadamente áreas públicas y restringidas.
- Evitar accesos no controlados.
- Crear zonas de transición.
- Proteger ductos, cielorrasos y cavidades utilizadas para ocultamiento.
- Facilitar inspecciones.
- Mantener visibilidad sobre rutas de circulación.

Los nuevos proyectos penitenciarios deberán incorporar estos requisitos desde su fase de diseño.

21. Inspecciones aleatorias internas

Además de los controles de entrada, se realizarán inspecciones internas aleatorias. Estas deberán diseñarse con criterios que impidan que los horarios puedan conocerse anticipadamente.

El propósito no será aumentar indiscriminadamente las requisas, sino reducir la previsibilidad del sistema.

Las inspecciones podrán apoyarse en inteligencia obtenida mediante cámaras, detectores y registros de incidentes.

22. Integridad de los procedimientos

RD Propone RD Propone

Los controles perderían eficacia si el propio personal pudiera desactivarlos informalmente, por tanto, ningún funcionario individual deberá tener capacidad para suspender arbitrariamente los controles de ingreso.

Toda excepción deberá quedar registrada. El sistema informático deberá conservar:

- Funcionario que autorizó la excepción.
- Persona beneficiada.
- Motivo.
- Fecha.
- Hora.
- Duración.

Esto permitirá auditar posteriormente decisiones excepcionales.

23. Supervisión cruzada

En puntos especialmente sensibles deberá procurarse que determinadas actuaciones requieran intervención o conocimiento de más de un funcionario. Por ejemplo, la recepción de una entrega excepcional o el ingreso de un dispositivo tecnológico no registrado podría requerir doble autorización.

Este mecanismo reduce el riesgo de que una sola persona pueda vulnerar el procedimiento.

24. Auditoría sorpresa

Los centros estarán sujetos a auditorías periódicas y no anunciadas. Equipos especializados podrán evaluar:

- Funcionamiento de los controles.
- Cumplimiento de protocolos.
- Existencia de puntos vulnerables.
- Funcionamiento de cámaras.
- Registros de accesos.
- Inventarios tecnológicos.
- Cumplimiento de la política de teléfonos del personal.

Los resultados deberán generar planes correctivos obligatorios.

25. Indicadores de desempeño

RD Propone RD Propone

La efectividad del sistema no deberá medirse únicamente por la cantidad de objetos decomisados. Deberán utilizarse indicadores como:

- Intentos detectados antes de ingresar.
- Dispositivos encontrados dentro del centro.
- Reincidencia por modalidad.
- Incidentes asociados a funcionarios.
- Áreas con mayor frecuencia de decomisos.
- Tiempo transcurrido entre detección e intervención.
- Cantidad de dispositivos autorizados dentro de cada establecimiento.

La evolución de estos indicadores permitirá determinar si las medidas están produciendo resultados.

26. Principio de adaptación tecnológica

Las modalidades de introducción evolucionan constantemente, por ello, la política deberá permitir actualizar protocolos, equipos y categorías de objetos prohibidos mediante disposiciones administrativas y técnicas, evitando que cada innovación tecnológica requiera una reforma legislativa completa.

La normativa deberá establecer principios generales suficientemente amplios para responder a nuevas tecnologías.

27. Resultado esperado

El Sistema de Prevención del Ingreso deberá transformar el acceso a los establecimientos penitenciarios en un proceso trazable, auditable y difícil de vulnerar. El objetivo no será multiplicar innecesariamente los controles, sino lograr que cualquier persona que pretenda introducir clandestinamente un dispositivo tenga que superar simultáneamente barreras humanas, físicas, tecnológicas y administrativas.

La seguridad comenzará antes de que el dispositivo alcance el interior del centro.

CAPÍTULO III
DETECCIÓN, LOCALIZACIÓN, DECOMISO Y TRAZABILIDAD DE DISPOSITIVOS ILÍCITOS

1. Objeto del capítulo

RD Propone RD Propone

El presente capítulo establece los lineamientos para detectar, localizar, decomisar, registrar y analizar los dispositivos tecnológicos no autorizados que hayan logrado superar los controles de ingreso de los centros penitenciarios.

La política reconoce que ningún mecanismo preventivo puede garantizar una eficacia absoluta. Por esta razón, la eventual penetración de un teléfono celular, tarjeta SIM, cargador, batería portátil u otro dispositivo no deberá significar automáticamente que este pueda ser utilizado libremente.

El sistema deberá procurar que cualquier dispositivo clandestino que alcance el interior del establecimiento deje rastros técnicos, físicos o administrativos que permitan elevar significativamente la probabilidad de su descubrimiento.

2. Principio de detección permanente

Cada centro deberá desarrollar capacidades permanentes para identificar indicios de dispositivos electrónicos clandestinos mediante la combinación de:

a) Información de inteligencia penitenciaria;

b) Sistemas de telecomunicaciones;

c) Videovigilancia;

d) Inspecciones físicas;

e) Equipos especializados de detección;

f) Análisis de patrones;

g) Información proveniente de decomisos anteriores;

h) Alertas sobre comportamientos o incidentes anormales.

Ninguna de estas herramientas deberá considerarse suficiente por sí sola.

3. División tecnológica del centro penitenciario

Cada establecimiento deberá elaborar un mapa digital de seguridad que permita dividir el recinto en sectores identificables. Podrán establecerse, entre otras:

a) Zona administrativa;

b) Zona médica;

RD Propone RD Propone

c) Área de visitas;

d) Bloques de alojamiento;

e) Talleres;

f) Áreas educativas;

g) Cocina;

h) Almacenes;

i) Áreas de recreación;

j) Perímetro exterior;

k) Áreas técnicas;

l) Zonas de carga y descarga.

Cada incidente deberá asociarse a una zona determinada.

El objetivo será evitar que la detección de una actividad clandestina obligue necesariamente a intervenir todo el establecimiento cuando existan medios razonables para delimitar el área probable.

4. Detección de actividad celular

En coordinación con INDOTEL y las prestadoras de servicios de telecomunicaciones, deberán implementarse mecanismos técnicamente autorizados que permitan conocer la existencia de dispositivos celulares no autorizados dentro del perímetro penitenciario. El sistema deberá diferenciar, cuando técnicamente resulte posible, entre:

- Dispositivos institucionales autorizados.
- Dispositivos de visitantes ubicados en zonas permitidas.
- Dispositivos pertenecientes a comunidades externas.
- Dispositivos sospechosos localizados dentro de áreas restringidas.

Toda tecnología empleada deberá configurarse procurando evitar afectaciones indebidas a usuarios legítimos situados fuera del establecimiento.

La regulación dominicana ya contempla desde 2011 el uso de equipos destinados a bloquear comunicaciones móviles desde centros penitenciarios, y posteriormente INDOTEL ha retomado programas de instalación de bloqueadores.

RD Propone RD Propone

5. Registro técnico del dispositivo detectado

Cuando técnicamente pueda identificarse un equipo sospechoso, deberán registrarse los datos permitidos por la legislación aplicable. Entre estos podrán incluirse:

a) Identificador técnico del terminal;

b) Identificación de la línea o servicio cuando legalmente corresponda;

c) Operadora asociada;

d) Fecha de detección;

e) Hora;

f) Zona aproximada;

g) Duración de la actividad;

h) Reincidencia del mismo dispositivo;

i) Relación con incidentes anteriores.

La información deberá utilizarse exclusivamente para fines legítimos de seguridad, investigación y administración penitenciaria.

6. Sistema de alertas

Las alertas podrán clasificarse según su nivel de riesgo. Por ejemplo:

Nivel 1: Detección aislada.

Nivel 2: Actividad repetitiva.

Nivel 3: Múltiples dispositivos en una misma zona.

Nivel 4: Actividad relacionada con información sobre posible conducta delictiva.

La clasificación servirá para determinar la intensidad y rapidez de la respuesta.

7. Inspecciones dirigidas

Las inspecciones internas deberán evolucionar progresivamente desde un modelo exclusivamente general hacia un modelo apoyado en inteligencia. Cuando exista una

RD Propone RD Propone

alerta técnicamente confiable sobre determinada zona, el personal podrá realizar inspecciones focalizadas conforme a los procedimientos establecidos.

Esto permitirá reducir intervenciones innecesariamente amplias y concentrar los recursos donde exista mayor probabilidad de encontrar dispositivos.

8. Uso de detectores electrónicos

Los centros podrán disponer de equipos especializados capaces de ayudar a identificar la presencia de componentes electrónicos. Su utilización podrá realizarse:

a) Durante inspecciones programadas;

b) Ante alertas específicas;

c) Durante auditorías sorpresa;

d) En áreas donde hayan ocurrido decomisos recurrentes;

e) Durante inspecciones posteriores a trabajos de mantenimiento o construcción.

Estos equipos deberán ser operados por personal debidamente capacitado.

9. Detección de cargadores, baterías y accesorios

La búsqueda no deberá concentrarse exclusivamente en el teléfono. Un sistema eficaz deberá localizar también los elementos necesarios para mantenerlo operativo.

Por tanto, las inspecciones deberán prestar atención particular a:

- Cargadores.
- Cables.
- Adaptadores.
- Baterías externas.
- Transformadores.
- Extensiones improvisadas.
- Conexiones eléctricas clandestinas.
- Componentes utilizados para modificar instalaciones eléctricas.

La aparición recurrente de estos elementos deberá generar revisiones sobre posibles fuentes de abastecimiento dentro del establecimiento.

10. Integración con videovigilancia

RD Propone RD Propone

Cuando una alerta tecnológica permita determinar aproximadamente la zona y hora de utilización de un dispositivo, el sistema deberá facilitar la revisión de las cámaras correspondientes. Por ejemplo:

Alerta tecnológica:

Centro:	XXX
Bloque:	B
Zona:	Segundo nivel
Hora inicial:	22:14
Hora final:	22:27

El sistema podría identificar automáticamente las cámaras existentes en esa área y marcar el intervalo correspondiente para revisión. Esto reduciría considerablemente el tiempo necesario para analizar grabaciones.

11. Analítica de video

De manera gradual podrán incorporarse herramientas de análisis automático de video destinadas a detectar comportamientos que ameriten revisión humana.

Estas herramientas no deberán determinar automáticamente responsabilidad disciplinaria o penal. Su función será identificar eventos que requieran evaluación.

Toda actuación posterior deberá ser realizada por personal competente y conforme a las garantías correspondientes.

12. Protección de espacios privados

La videovigilancia deberá respetar áreas en las cuales la intimidad resulte especialmente protegida. No deberán utilizarse cámaras de manera indiscriminada en:

- Baños.
- Duchas.
- Áreas destinadas a consultas médicas privadas.
- Espacios destinados a comunicaciones legalmente protegidas con abogados.
- Otros lugares donde la captación permanente resulte incompatible con derechos fundamentales.

La seguridad deberá diseñarse de manera que no convierta la vigilancia tecnológica en un mecanismo de observación absoluta de la vida de las personas privadas de libertad.

RD Propone RD Propone

13. Procedimiento de decomiso

Todo dispositivo localizado deberá ser inmediatamente asegurado conforme a un procedimiento uniforme. El funcionario actuante deberá registrar:

a) Fecha;
b) Hora;
c) Lugar exacto;
d) Tipo de dispositivo;
e) Marca y modelo cuando sea identificable;
f) Estado físico;
g) Persona a quien se atribuya inicialmente la posesión, cuando corresponda;
h) Funcionarios presentes;
i) Fotografías del hallazgo;
j) Número de identificación del registro.
La documentación deberá iniciarse en el mismo momento del decomiso.

14. Prohibición de manipulación innecesaria

El teléfono decomisado no deberá ser manipulado arbitrariamente por múltiples funcionarios. Cuando existan indicios de que pueda contener evidencia relacionada con hechos delictivos, deberá preservarse conforme a procedimientos de cadena de custodia.

El personal penitenciario no deberá revisar informalmente comunicaciones, fotografías o contenidos almacenados cuando esto requiera autorización legal o judicial.

15. Cadena de custodia

Los dispositivos relacionados con posibles investigaciones criminales deberán tratarse como potencial evidencia. Se deberá documentar:

- Quién lo encontró.
- Quién lo recibió.
- Dónde fue almacenado.
- Cada traslado realizado.
- Cada funcionario que tuvo acceso.
- Fecha y hora de cada movimiento.
- Autoridad a la que fue entregado.

RD Propone RD Propone

Esto reducirá la posibilidad de sustitución, pérdida, manipulación o desaparición de evidencias.

16. Registro Nacional de Dispositivos Penitenciarios Decomisados

Se creará una base de datos nacional que permita registrar los dispositivos tecnológicos encontrados en todos los establecimientos penitenciarios.

El registro permitirá relacionar incidentes producidos en diferentes fechas o centros.

Cuando sea legal y técnicamente posible, se almacenarán identificadores que permitan reconocer si un mismo teléfono, SIM u otro componente ha aparecido anteriormente.

17. Cruce de información

El verdadero valor de la base de datos no radicará únicamente en almacenar decomisos, el sistema deberá poder identificar coincidencias. Por ejemplo:

- Un mismo identificador técnico detectado en distintas fechas.
- SIM relacionadas con varios dispositivos.
- Múltiples teléfonos encontrados en una misma zona.
- Incidentes vinculados a determinados horarios.
- Repetición de decomisos durante turnos específicos.
- Dispositivos asociados recurrentemente a determinados métodos de introducción.

Estas coincidencias no constituirán por sí mismas prueba de responsabilidad, pero podrán generar líneas de investigación.

18. Mapa nacional de incidentes

La autoridad penitenciaria deberá disponer de un tablero nacional que permita visualizar el comportamiento del problema. Podrá mostrar, entre otros indicadores:

- Número de dispositivos decomisados por centro.
- Tipo de dispositivo.
- Zona del establecimiento.
- Método probable de ingreso.
- Cantidad de SIM.
- Cantidad de cargadores.
- Incidentes vinculados a empleados o visitantes.
- Reincidencias.

RD Propone RD Propone

- Variación mensual.

El objetivo será convertir una serie de decomisos aislados en inteligencia institucional.

19. Identificación de centros de mayor riesgo

A partir de los datos recopilados se podrán clasificar los establecimientos según niveles de incidencia. Esta clasificación permitirá decidir dónde priorizar:

- Tecnología.
- Personal especializado.
- Auditorías.
- Remodelaciones.
- Capacitación.
- Investigaciones internas.

La asignación de recursos deberá basarse progresivamente en evidencia.

20. Indicador de densidad tecnológica ilícita

La política podrá desarrollar un indicador que relacione:

- Cantidad de internos.
- Cantidad de dispositivos encontrados.
- Actividad celular no autorizada detectada.
- Cantidad de incidentes.
- Reincidencia.
- Este indicador permitirá comparar centros de distintos tamaños.

No deberá utilizarse automáticamente para sancionar administraciones penitenciarias, debido a que un mayor número de decomisos también podría ser consecuencia de mejores mecanismos de detección.

21. Inteligencia sobre rutas de introducción

Cada teléfono decomisado deberá generar una investigación administrativa mínima orientada a determinar cómo pudo ingresar. No siempre será posible establecerlo, sin embargo, cuando múltiples dispositivos presenten patrones similares podrá identificarse una ruta. Por ejemplo:

- Mercancías.
- Visitas.

RD Propone RD Propone

- Personal.
- Trabajos técnicos.
- Lanzamientos desde el exterior.
- Vehículos.
- Encomiendas.
- Otros mecanismos.

Una ruta detectada deberá generar ajustes inmediatos en los protocolos correspondientes.

22. Investigación sobre corrupción interna

Cuando los patrones indiquen posible participación del personal, deberá activarse un protocolo especial de investigación. La información deberá remitirse a las unidades competentes.

Ningún funcionario deberá ser considerado responsable exclusivamente por coincidir con determinados horarios o incidentes.

Los patrones tecnológicos constituirán herramientas de investigación, no sustitutos del debido proceso.

23. Conservación y protección de datos

Las bases de datos generadas deberán protegerse mediante controles de acceso. No todo funcionario tendrá acceso a toda la información.

Los permisos deberán asignarse según función. El sistema deberá registrar:

- Quién consultó la información.
- Qué expediente consultó.
- Cuándo.
- Qué modificación realizó.

Las consultas deberán ser auditables.

24. Centro Nacional de Monitoreo Penitenciario

Se establecerá progresivamente una capacidad nacional de monitoreo desde donde pueda observarse el estado tecnológico de los establecimientos. Este centro podrá recibir información sobre:

RD Propone RD Propone

Alertas de dispositivos.
Estado de sistemas de bloqueo.
Incidentes.
Equipos fuera de servicio.
Patrones anormales.
Resultados de auditorías.
El centro no sustituirá la autoridad de cada establecimiento, sino que permitirá coordinación, supervisión y análisis nacional.

25. Protocolo de respuesta

Toda alerta deberá conducir a una actuación preestablecida. El protocolo deberá indicar:

- Quién recibe la alerta.
- Quién valida.
- Quién autoriza intervención.
- Qué personal participa.
- Cómo se documenta.
- Qué ocurre si se encuentra un dispositivo.
- Qué ocurre si no se encuentra.
- Cómo se cierra el incidente.

Esto evitará que las alertas dependan únicamente de decisiones improvisadas.

26. Indicadores de efectividad

Se deberán medir periódicamente:

- Tiempo promedio entre detección e intervención.
- Porcentaje de alertas verificadas.
- Cantidad de dispositivos recuperados.
- Reincidencia de identificadores.
- Cantidad de rutas de ingreso descubiertas.
- Zonas con mayor concentración.
- Cantidad de investigaciones derivadas.
- Cantidad de alertas falsas.

27. Auditoría tecnológica

RD Propone RD Propone

Los equipos técnicos podrán simular determinados escenarios mediante dispositivos autorizados para verificar:

- Capacidad de detección.
- Tiempo de respuesta.
- Cobertura tecnológica.
- Funcionamiento de cámaras.
- Funcionamiento de sistemas de alerta.
- Coordinación entre unidades.

Los dispositivos utilizados para las pruebas deberán estar identificados previamente para evitar confusión con equipos clandestinos.

28. Principio de aprendizaje institucional

Cada decomiso deberá considerarse no solamente una infracción detectada, sino una oportunidad para fortalecer el sistema. Después de incidentes significativos deberá responderse al menos a cuatro preguntas:

- ¿Cómo entró?
- ¿Cómo permaneció oculto?
- ¿Cómo obtuvo energía?
- ¿Cómo consiguió comunicarse?

La respuesta a estas preguntas deberá traducirse en medidas correctivas.

29. Resultado esperado

El objetivo final será transformar el interior del centro penitenciario en un ambiente tecnológicamente hostil para las comunicaciones clandestinas.

Un dispositivo que consiga superar la barrera de entrada deberá enfrentar detección electrónica, vigilancia, controles físicos, limitaciones de energía, restricciones de telecomunicaciones y análisis de patrones. La meta no será únicamente decomisar teléfonos.

Será conseguir que cada utilización clandestina incremente la posibilidad de localización del dispositivo, identificación de su ruta de entrada y descubrimiento de las personas vinculadas con su introducción o utilización.

CAPÍTULO IV

RD Propone RD Propone

NEUTRALIZACIÓN DE SEÑAL Y CONTROL DE TELECOMUNICACIONES PENITENCIARIAS

1. Objeto del capítulo

El presente capítulo establece los lineamientos para impedir o reducir significativamente la utilización de redes públicas de telecomunicaciones por parte de dispositivos no autorizados ubicados dentro de centros penitenciarios.

La política reconoce que la neutralización efectiva de las comunicaciones ilícitas no debe depender exclusivamente de inhibidores convencionales de señal, sino de una combinación de tecnologías que permitan bloquear, identificar, clasificar y administrar las conexiones dentro de los perímetros penitenciarios.

El sistema deberá procurar simultáneamente tres objetivos:

a) Impedir comunicaciones clandestinas desde las áreas restringidas;

b) Mantener disponibles las comunicaciones institucionales y de emergencia;

c) Evitar afectaciones injustificadas a usuarios y comunidades situadas fuera de los centros penitenciarios.

2. Autoridad reguladora

El Instituto Dominicano de las Telecomunicaciones deberá ejercer las funciones regulatorias y técnicas correspondientes dentro de sus competencias sobre redes, servicios y utilización del espectro radioeléctrico.

Toda solución destinada a interferir, restringir, administrar o modificar el acceso a redes móviles deberá implementarse conforme a la Ley General de Telecomunicaciones núm. 153-98 y a las disposiciones regulatorias emitidas por INDOTEL.

La Ley 153-98 constituye el marco básico para la instalación, mantenimiento y operación de redes, prestación de servicios y provisión de equipos de telecomunicaciones en el territorio dominicano.

3. Principio de neutralización selectiva

La política procurará evitar, siempre que la tecnología disponible lo permita, el bloqueo indiscriminado de todas las comunicaciones.

El objetivo será evolucionar hacia un modelo capaz de diferenciar entre:

RD Propone RD Propone

a) Comunicaciones institucionales autorizadas;

b) Servicios de emergencia;

c) Dispositivos oficialmente registrados;

d) Equipos pertenecientes a usuarios situados fuera del perímetro;

e) Dispositivos no autorizados dentro de áreas penitenciarias.

La arquitectura deberá favorecer soluciones de precisión sobre soluciones indiscriminadas.

4. Bloqueadores de señal

Los centros podrán utilizar sistemas de inhibición o bloqueo de señal cuando su instalación se encuentre técnicamente autorizada. Estos equipos deberán configurarse exclusivamente para cubrir las áreas necesarias. No deberán instalarse sin estudios previos de:

- Cobertura.
- Potencia.
- Frecuencias.
- Arquitectura del establecimiento.
- Localización de antenas de operadores.
- Comunidades vecinas.
- Servicios públicos próximos.
- Posibles interferencias.

El objetivo será impedir que el bloqueo exceda innecesariamente el perímetro del establecimiento.

5. Estudios radioeléctricos previos

Antes de instalar un sistema de bloqueo deberá realizarse un estudio técnico del entorno radioeléctrico. El estudio deberá identificar:

a) Operadoras presentes;

b) Bandas de frecuencia utilizadas;

c) Intensidad de señal;

d) Ubicación aproximada de estaciones base;

RD Propone RD Propone

e) Características constructivas del establecimiento;

f) Áreas internas de mayor vulnerabilidad;

g) Viviendas, empresas y servicios cercanos que pudieran resultar afectados.

Las soluciones deberán diseñarse individualmente para cada centro.

6. Acceso administrado

La política deberá evaluar e incorporar progresivamente sistemas de acceso administrado. Estos sistemas procurarán identificar los dispositivos que intentan acceder a las redes móviles dentro del perímetro y permitir únicamente aquellos previamente autorizados. El principio será:

No todo teléfono ubicado dentro de una cárcel será tratado de la misma manera; solamente los dispositivos expresamente autorizados podrán mantener determinadas comunicaciones.

7. Lista blanca nacional

Se creará una lista nacional de dispositivos autorizados. Podrán incluirse:

a) Equipos de dirección penitenciaria;

b) Dispositivos oficiales de seguridad;

c) Equipos médicos;

d) Terminales utilizados para emergencias;

e) Equipos técnicos de mantenimiento autorizados temporalmente;

f) Otros dispositivos institucionales debidamente justificados.

La autorización deberá ser individualizada.

8. Datos asociados a dispositivos autorizados

Cada dispositivo autorizado deberá registrar, cuando sea técnicamente posible:

- Nombre del responsable.
- Institución.
- Número telefónico.
- IMEI.
- Identificador de SIM.

RD Propone RD Propone

- Marca.
- Modelo.
- Centro autorizado.
- Zona autorizada.
- Horario permitido.
- Fecha de vencimiento.

La pérdida, sustitución o cambio del equipo deberá notificarse inmediatamente.

9. Autorizaciones temporales

Cuando contratistas, técnicos, investigadores u otras personas necesiten ingresar con equipos de comunicación, podrán emitirse autorizaciones temporales. Estas deberán expirar automáticamente.

La autorización no deberá permanecer activa después de finalizar el trabajo correspondiente.

10. Identificación de dispositivos desconocidos

Cuando un terminal no incluido en la lista autorizada intente conectarse dentro de una zona restringida, el sistema deberá generar una alerta. Siempre que resulte técnica y jurídicamente permitido, podrá registrarse:

- Identificador técnico.
- Fecha.
- Hora.
- Zona.
- Operadora.
- Frecuencia de aparición.
- Duración aproximada.

La identificación no implicará por sí misma una atribución de responsabilidad personal.

11. Lista de observación

Los dispositivos detectados repetidamente podrán incorporarse a una lista de observación. Esta lista servirá para determinar si:

a) El mismo equipo reaparece;

b) Cambia de ubicación dentro del centro;

RD Propone RD Propone

c) Aparece en diferentes centros penitenciarios;

d) Utiliza diferentes tarjetas SIM;

e) Está relacionado con incidentes anteriores.

El objetivo será facilitar investigaciones y análisis de patrones.

12. Coordinación con las prestadoras

Las empresas prestadoras de servicios móviles deberán participar mediante protocolos técnicos establecidos con INDOTEL. La coordinación podrá incluir mecanismos para:

a) Verificar información técnica;

b) Analizar interferencias;

c) Corregir zonas de cobertura no deseadas;

d) Aplicar medidas autorizadas sobre líneas o terminales relacionados con actividades ilícitas;

e) Mantener servicios esenciales;

f) Resolver afectaciones a comunidades vecinas.

Toda intervención sobre usuarios o servicios deberá realizarse conforme al marco legal correspondiente.

13. Neutralización por terminal

La política deberá evaluar mecanismos jurídicos y técnicos que permitan actuar no solamente sobre la señal general, sino sobre determinados terminales identificados.

Cuando existan fundamentos legales suficientes y confirmación técnica, podrá estudiarse la aplicación de medidas destinadas a impedir que determinados dispositivos continúen accediendo a redes móviles.

Estos mecanismos deberán estar sujetos a procedimientos previamente regulados y a controles contra errores o abusos.

14. Neutralización por línea

De igual manera, cuando una línea haya sido identificada conforme a los procedimientos legales aplicables como instrumento utilizado reiteradamente para comunicaciones

RD Propone RD Propone

ilícitas desde un centro penitenciario, podrán aplicarse las medidas que permita el ordenamiento jurídico. La política deberá establecer claramente:

- Quién solicita.
- Quién valida.
- Qué autoridad autoriza.
- Qué evidencia técnica se requiere.
- Cómo se ejecuta.
- Cómo puede revisarse una decisión errónea.

15. Prohibición de bloqueo automático sin verificación

La mera detección técnica no deberá producir automáticamente la cancelación definitiva de una línea o terminal. Deberá existir verificación.

Esto será especialmente importante en centros situados cerca de zonas residenciales donde una señal legítima pueda ser detectada desde el perímetro.

16. Sistemas redundantes

La arquitectura no deberá depender de un único equipo, cuando sea viable se utilizarán mecanismos complementarios. Por ejemplo:

- Bloqueo localizado.
- Acceso administrado.
- Detección de terminales.
- Monitoreo.
- Lista blanca.
- Auditoría de cobertura.

La falla de una tecnología no deberá dejar automáticamente al centro sin protección.

17. Monitoreo del funcionamiento

El Centro Nacional de Monitoreo podrá conocer:

- Equipo activo.
- Equipo fuera de servicio.
- Falla de energía.
- Falla de comunicación.
- Alteración física.

RD Propone RD Propone

- Cambio de configuración.
- Cobertura anormal.

El objetivo será evitar que un bloqueador permanezca fuera de servicio durante días sin conocimiento de las autoridades.

18. Protección contra manipulación

Los equipos de control de telecomunicaciones deberán ubicarse en espacios protegidos. El acceso deberá estar restringido a personal técnico autorizado.

Las modificaciones de configuración deberán quedar registradas. El sistema deberá identificar:

- Usuario.
- Fecha.
- Hora.
- Cambio realizado.
- Motivo.

Esto permitirá detectar posibles manipulaciones internas.

19. Energía de respaldo

Un corte de energía no deberá significar automáticamente la restauración de comunicaciones clandestinas. Los centros deberán evaluar baterías, sistemas UPS u otras soluciones apropiadas según su infraestructura.

20. Pruebas periódicas

No será suficiente asumir que un equipo funciona porque aparece encendido. Deberán realizarse pruebas controladas.

Equipos técnicos autorizados podrán ingresar con terminales previamente registrados y verificar:

- Llamadas.
- Mensajes.
- Datos móviles.
- Conexiones en distintas zonas.
- Comportamiento de diferentes operadoras.

RD Propone RD Propone

El resultado deberá documentarse.

21. Mapas de cobertura penitenciaria

Cada centro deberá mantener un mapa actualizado de cobertura. Este permitirá identificar:

- Áreas completamente neutralizadas.
- Áreas parcialmente neutralizadas.
- Zonas donde exista fuga de señal.
- Zonas donde el bloqueo se extienda excesivamente.

Estos mapas deberán actualizarse después de remodelaciones importantes o cambios en redes móviles externas.

22. Protección de comunidades cercanas

Una de las principales exigencias de la política será evitar que las medidas penitenciarias afecten injustificadamente a terceros. Si residentes o empresas cercanas presentan interrupciones derivadas de sistemas penitenciarios, deberá existir un mecanismo de reporte e investigación.

INDOTEL deberá poder verificar técnicamente la reclamación y ordenar los ajustes necesarios.

23. Servicios de emergencia

La arquitectura deberá prever comunicaciones para:

- Emergencias médicas.
- Bomberos.
- Seguridad.
- Protección Civil.
- Autoridades penitenciarias.
- Otros servicios esenciales.

Cuando el bloqueo pudiera afectar estas comunicaciones deberán diseñarse canales alternativos seguros.

24. Comunicación institucional interna

RD Propone RD Propone

Los centros no deberán depender necesariamente de teléfonos celulares comerciales para todas sus comunicaciones. Podrán utilizar:

- Radios institucionales.
- Redes privadas.
- Telefonía fija.
- Sistemas internos cifrados.
- Terminales especialmente autorizados.

Esto reducirá la necesidad de mantener excepciones amplias dentro de las zonas restringidas.

25. Actualización tecnológica

Los sistemas adquiridos deberán ser capaces de adaptarse a nuevas generaciones tecnológicas. Las especificaciones de contratación deberán evitar adquirir soluciones cuya eficacia desaparezca rápidamente ante cambios en frecuencias o tecnologías.

26. Contrataciones tecnológicamente neutrales

Los procesos de adquisición no deberán diseñarse alrededor de una única marca o fabricante. Los pliegos deberán establecer resultados esperados. Por ejemplo:

- Porcentaje de cobertura.
- Capacidad de detección.
- Precisión.
- Disponibilidad.
- Interoperabilidad.
- Mantenimiento.
- Actualización.
- Seguridad informática.

Esto permitirá comparar soluciones competitivas.

27. Pruebas antes de aceptación

Antes de recibir definitivamente cualquier sistema, deberá realizarse una prueba de aceptación técnica. La prueba deberá comprobar el funcionamiento real dentro del centro. El pago final podrá condicionarse al cumplimiento de parámetros previamente establecidos.

RD Propone RD Propone

28. Mantenimiento obligatorio

La adquisición de equipos sin mantenimiento deberá evitarse. El contrato deberá contemplar:

- Tiempo máximo de respuesta.
- Disponibilidad de repuestos.
- Actualizaciones.
- Soporte técnico.
- Capacitación.
- Garantías.

29. Auditoría independiente

Las auditorías podrán ser realizadas por unidades técnicas acreditadas o equipos públicos especializados. La independencia de la evaluación permitirá evitar que la institución responsable se evalúe exclusivamente a sí misma.

30. Indicadores nacionales

El sistema deberá medir:

- Porcentaje de centros protegidos.
- Porcentaje de áreas cubiertas.
- Cantidad de terminales no autorizados detectados.
- Reincidencia de dispositivos.
- Tiempo promedio de neutralización.
- Número de fallas técnicas.
- Duración promedio de fallas.
- Quejas por interferencias externas.
- Resultados de pruebas sorpresa.

31. Relación con el programa existente

La política deberá incorporar y evaluar los programas de bloqueadores ya desarrollados o financiados por el Estado dominicano. INDOTEL informó oficialmente la puesta en marcha de bloqueadores en centros penitenciarios y el inicio de un plan piloto en La Vega.

La nueva política no deberá duplicar inversiones funcionales. Deberá determinar qué equipos ya existen, dónde están instalados, qué tecnología utilizan, cuál es su estado y cuáles han sido sus resultados.

RD Propone RD Propone

32. Evaluación del piloto de La Vega

Antes de expandir de manera definitiva un modelo nacional, deberá documentarse técnicamente la experiencia del plan piloto iniciado en La Vega. La evaluación deberá determinar:

- Cobertura obtenida.
- Operadoras afectadas.
- Incidencias técnicas.
- Quejas externas.
- Costos.
- Mantenimiento.
- Cantidad de comunicaciones detectadas antes y después.
- Cantidad de dispositivos decomisados.
- Fallos encontrados.
- Mejoras necesarias.

Los resultados deberán servir como insumo para el diseño nacional.

33. Fondo para seguridad tecnológica penitenciaria

Podrá estructurarse un mecanismo presupuestario específico para adquisición, actualización, mantenimiento y auditoría de tecnologías de neutralización.

Los recursos deberán estar sometidos a controles de ejecución y resultados.

La inversión no deberá evaluarse simplemente por monto gastado, sino por reducción comprobable de capacidad de comunicación clandestina.

34. Coordinación nacional

Se establecerá una mesa técnica permanente integrada, como mínimo, por:

- Ministerio de Justicia.
- Autoridad penitenciaria.
- INDOTEL.
- Prestadoras de telecomunicaciones.
- Autoridades de seguridad e investigación según corresponda.
- Unidades técnicas especializadas.

La mesa deberá evaluar periódicamente nuevas vulnerabilidades y tecnologías.

RD Propone RD Propone

35. Principio de confidencialidad operacional

Determinados parámetros técnicos relacionados con cobertura, configuración o vulnerabilidades no deberán hacerse públicos cuando su divulgación facilite mecanismos de evasión. Esto no impedirá la transparencia sobre:

- Contrataciones.
- Costos.
- Indicadores.
- Resultados generales.
- Auditorías.
- Cumplimiento.

La política deberá distinguir entre transparencia administrativa y protección legítima de información operacional sensible.

36. Resultado esperado

La finalidad será que un teléfono clandestino que consiga ingresar a un centro penitenciario no pueda asumir que encontrará libre acceso a una red móvil.

El sistema deberá convertir el entorno penitenciario en un espacio donde las comunicaciones inalámbricas se encuentren *administradas, verificadas, monitoreadas y técnicamente controladas.*

El éxito no deberá medirse únicamente por la cantidad de señal bloqueada, sino por la reducción real y comprobable de comunicaciones ilícitas sin perjudicar indebidamente los derechos de terceros ni los servicios esenciales.

CAPÍTULO V
SEGURIDAD ELÉCTRICA PENITENCIARIA Y CONTROL DE LA CAPACIDAD DE CARGA DE DISPOSITIVOS NO AUTORIZADOS

1. Objeto del capítulo

El presente capítulo establece los lineamientos para incorporar la infraestructura eléctrica de los centros penitenciarios como una capa adicional del sistema de prevención y neutralización de comunicaciones ilícitas.

La política parte de una realidad operativa básica: cualquier teléfono celular, dispositivo de comunicación, batería portátil o equipo electrónico clandestino necesita obtener energía periódicamente para mantenerse operativo.

RD Propone RD Propone

Por tanto, aun cuando un dispositivo consiga superar los controles de entrada, permanecer oculto y acceder temporalmente a una red de telecomunicaciones, deberá encontrarse con dificultades adicionales para obtener energía de forma clandestina.

El propósito será reducir las posibilidades de carga no autorizada sin afectar la iluminación, ventilación, refrigeración, servicios médicos, equipos de seguridad, instalaciones educativas, servicios sanitarios u otras necesidades legítimas del establecimiento.

2. Principio de seguridad eléctrica penitenciaria

Los centros penitenciarios deberán incorporar progresivamente un concepto de *seguridad eléctrica penitenciaria.*

Este concepto comprenderá el diseño, instalación, distribución, protección, monitoreo y mantenimiento de los sistemas eléctricos tomando en consideración no solamente criterios tradicionales de funcionamiento y seguridad, sino también los riesgos derivados de su utilización para alimentar dispositivos tecnológicos no autorizados.

Las instalaciones deberán diseñarse de forma que dificulten la manipulación, alteración o utilización clandestina de los puntos eléctricos.

3. Prohibición de mecanismos destinados a dañar dispositivos

Quedará descartada la utilización deliberada de sobretensiones, alteraciones peligrosas de voltaje, descargas eléctricas, modificaciones irregulares de frecuencia u otros mecanismos destinados específicamente a destruir teléfonos celulares u otros dispositivos conectados.

La infraestructura eléctrica penitenciaria deberá respetar las normas de seguridad eléctrica y protección contra incendios aplicables.

El objetivo será *controlar el acceso a la energía*, no convertir la instalación eléctrica en un mecanismo de destrucción de equipos.

4. Reducción de tomacorrientes de libre acceso

Las áreas destinadas al alojamiento permanente de personas privadas de libertad deberán reducir progresivamente la existencia de tomacorrientes convencionales de libre acceso cuando estos no resulten necesarios para necesidades legítimas.

Esta reducción deberá realizarse mediante estudios técnicos previos.

RD Propone RD Propone

No deberán eliminarse conexiones necesarias para condiciones mínimas de habitabilidad, seguridad, salud o programas institucionales.

5. Separación de circuitos

Las instalaciones eléctricas deberán procurar una separación funcional entre:

a) Iluminación;

b) Ventilación;

c) Seguridad;

d) Equipos médicos;

e) Sistemas tecnológicos;

f) Equipos de cocina;

g) Servicios administrativos;

h) Tomas de uso general;

i) Sistemas críticos.

Esta separación permitirá controlar determinados circuitos sin afectar servicios esenciales.

6. Tomacorrientes penitenciarios protegidos

Cuando resulte necesario disponer de tomacorrientes dentro de áreas restringidas, estos deberán utilizar diseños físicamente resistentes a manipulación. Podrán incorporarse:

a) Cubiertas de seguridad;

b) Cajas metálicas protegidas;

c) Tornillería especial;

d) Sistemas empotrados;

e) Mecanismos que dificulten conexiones improvisadas;

f) Interruptores protegidos;

g) Otras soluciones técnicamente certificadas.

RD Propone RD Propone

El objetivo será evitar que un tomacorriente pueda modificarse fácilmente para realizar conexiones clandestinas.

7. Tomas eléctricas controladas

Los centros podrán implementar progresivamente puntos eléctricos cuyo funcionamiento pueda ser administrado. Estos podrán disponer de:

a) Activación programada;

b) Desactivación automática;

c) Control desde sistemas centrales;

d) Monitoreo de consumo;

e) Registro de funcionamiento;

f) Protección contra manipulación.

Su utilización deberá determinarse mediante estudio de ingeniería.

8. Temporización de determinados circuitos

En áreas donde existan tomacorrientes destinados a actividades específicas, podrá establecerse funcionamiento durante períodos determinados. Por ejemplo, determinados circuitos podrán encontrarse activos únicamente durante actividades educativas, laborales o recreativas autorizadas.

Al concluir la actividad, el circuito podrá desactivarse automáticamente, esto reducirá la disponibilidad permanente de energía para usos clandestinos.

9. Control nocturno

El diseño eléctrico deberá prestar especial atención a períodos durante los cuales determinadas instalaciones no requieren alimentación de tomas generales. Cuando resulte técnicamente apropiado y no afecte condiciones legítimas de habitabilidad, ciertos circuitos podrán limitarse durante horarios nocturnos.

La iluminación, ventilación, sistemas de emergencia y demás servicios esenciales deberán permanecer garantizados.

10. Monitoreo de consumo eléctrico

RD Propone RD Propone

Los centros penitenciarios podrán incorporar sistemas capaces de observar el consumo eléctrico por zonas o circuitos. El objetivo será establecer patrones normales de consumo.

Cuando se produzcan desviaciones significativas o comportamientos eléctricos anormales, el sistema podrá generar una alerta técnica para revisión.

Una anomalía eléctrica no constituirá por sí misma prueba de posesión de un dispositivo prohibido. Será únicamente un indicador que podrá justificar una inspección técnica.

11. Submedición por áreas

En establecimientos de mayor tamaño podrá evaluarse la instalación de submedidores. Estos permitirán conocer el consumo por:

- Bloque.
- Nivel.
- Área.
- Taller.
- Zona común.
- Sector administrativo.

La información permitirá identificar áreas donde existan desviaciones recurrentes.

12. Alertas de consumo anormal

El sistema podrá generar alertas cuando existan consumos incompatibles con el funcionamiento esperado de determinado circuito.

Por ejemplo, un circuito destinado únicamente a iluminación podría mostrar un comportamiento distinto al patrón normal.

La alerta deberá ser revisada por personal técnico antes de asumir cualquier irregularidad.

13. Prohibición de conexiones improvisadas

Se establecerá una política estricta contra:

- Extensiones no autorizadas.
- Empalmes.
- Conexiones desde luminarias.
- Manipulación de cajas eléctricas.

RD Propone RD Propone

- Alteración de interruptores.
- Conexiones a motores o ventiladores.
- Derivaciones desde equipos institucionales.

Cualquier intervención deberá ser realizada exclusivamente por personal técnico autorizado.

14. Inspección periódica de instalaciones

Las inspecciones deberán procurar identificar:

a) Manipulaciones;

b) Sellos rotos;

c) Tornillos removidos;

d) Conductores modificados;

e) Cables añadidos;

f) Adaptadores improvisados;

g) Daños deliberados;

h) Derivaciones no registradas.

Toda modificación deberá investigarse y corregirse.

15. Sellos de seguridad

Determinadas cajas eléctricas, paneles y puntos especialmente vulnerables podrán utilizar sellos numerados o mecanismos equivalentes.

Durante cada inspección podrá verificarse si el sello permanece intacto. La ruptura deberá quedar registrada.

Este procedimiento permitirá identificar manipulaciones aun cuando posteriormente se intente restaurar físicamente la instalación.

16. Registro de mantenimiento

El registro deberá indicar:

- Fecha.
- Hora.

RD Propone RD Propone

- Área.
- Trabajo realizado.
- Técnico responsable.
- Empresa, cuando corresponda.
- Componentes sustituidos.
- Motivo de intervención.
- Hora de salida.

Esto permitirá diferenciar trabajos legítimos de manipulaciones no autorizadas.

17. Control de herramientas eléctricas

Las herramientas utilizadas para mantenimiento deberán inventariarse al ingresar. Taladros, cables, adaptadores, extensiones, cargadores, medidores y demás herramientas susceptibles de dejar componentes aprovechables deberán comprobarse nuevamente al finalizar el trabajo.

No deberá permitirse que materiales eléctricos permanezcan abandonados dentro de áreas restringidas.

18. Control de cargadores

Ningún cargador particular deberá ingresar a las áreas de internos salvo autorización expresa. Los cargadores institucionales deberán registrarse e identificarse.

La aparición de un cargador clandestino deberá investigarse con la misma atención que la aparición de un teléfono.

19. Control de cables

Los cables USB y equivalentes deberán incluirse expresamente dentro de los objetos tecnológicos controlados.

Esto responde a que un teléfono puede obtener energía mediante múltiples fuentes aun cuando no exista un cargador convencional.

Los controles de acceso deberán prestar atención a cables aparentemente ordinarios que puedan utilizarse para carga o transferencia de datos.

20. Control de baterías portátiles

RD Propone RD Propone

Las baterías externas o bancos de energía deberán considerarse elementos de alto interés de seguridad.

Una batería portátil puede permitir mantener un teléfono funcionando durante períodos prolongados sin necesidad de acceder inmediatamente a un tomacorriente.

Su ingreso a áreas restringidas deberá requerir autorización específica.

21. Control de baterías de otros equipos

La política deberá reconocer que una persona puede intentar obtener energía desde equipos que originalmente tienen otra función. Por tanto, deberán evaluarse los riesgos asociados con baterías pertenecientes a:

- Radios.
- Herramientas.
- Equipos médicos.
- Equipos de limpieza.
- Lámparas.
- Sistemas portátiles.
- Otros dispositivos institucionales.

Esto no implica prohibirlos, sino controlar su disponibilidad y trazabilidad.

22. Equipos institucionales de carga

Los equipos oficiales utilizados dentro del establecimiento deberán disponer de puntos de carga institucionales. Estos puntos podrán ubicarse en áreas controladas.

De esta manera se reduce la necesidad de mantener tomacorrientes de libre utilización dentro de espacios sensibles.

23. Estaciones de carga autorizada

Cuando los programas penitenciarios legítimos requieran utilizar tablets, computadoras portátiles u otros dispositivos educativos, podrán establecerse estaciones específicas de carga. Estas estaciones deberán permitir únicamente equipos autorizados.

Su funcionamiento podrá limitarse a determinados horarios y permanecer bajo supervisión.

24. Dispositivos educativos institucionales

RD Propone RD Propone

Las personas privadas de libertad podrán utilizar equipos educativos, laborales o de rehabilitación cuando estén institucionalmente autorizados. Estos dispositivos deberán estar:

- Registrados.
- Inventariados.
- Configurados.
- Supervisados.
- Limitados a las funciones previstas.

La seguridad contra celulares clandestinos no deberá convertirse en una barrera injustificada para la educación digital.

25. Diseño de nuevas prisiones

Todo nuevo establecimiento penitenciario deberá incorporar la seguridad eléctrica desde su diseño. Los planos deberán evitar:

- Tomacorrientes innecesarios.
- Canalizaciones fácilmente accesibles.
- Cajas manipulables.
- Cableados expuestos.
- Paneles ubicados en áreas no controladas.
- Espacios que permitan conexiones clandestinas.

El diseño inicial será generalmente más eficiente que intentar corregir posteriormente instalaciones vulnerables.

26. Adecuación progresiva de centros existentes

Los establecimientos actuales deberán someterse a evaluaciones de vulnerabilidad eléctrica. La transformación podrá realizarse por etapas. Se priorizarán:

a) Centros con mayor número de decomisos;

b) Bloques con incidentes recurrentes;

c) Instalaciones antiguas;

d) Áreas con tomacorrientes de libre acceso;

e) Zonas donde se hayan encontrado conexiones clandestinas.

RD Propone RD Propone

Esto permitirá administrar razonablemente los costos.

27. Mapa eléctrico de seguridad

Cada establecimiento deberá disponer de un mapa actualizado de su infraestructura eléctrica. El mapa identificará:

- Paneles.
- Circuitos.
- Tomacorrientes.
- Áreas críticas.
- Equipos esenciales.
- Zonas de riesgo.
- Puntos de desconexión.

La información técnica deberá protegerse para evitar que pueda utilizarse para vulnerar el sistema.

28. Integración con el sistema de alertas penitenciarias

Las alertas eléctricas podrán integrarse con otros sistemas de seguridad. Por ejemplo:

Zona B: consumo eléctrico anormal.

Si simultáneamente existe:

Zona B: dispositivo móvil no autorizado detectado.

El sistema podrá elevar el nivel de riesgo del incidente. Esto permitirá combinar diferentes fuentes de información.

29. Correlación de eventos

El Centro Nacional de Monitoreo podrá utilizar información proveniente de:

- Actividad celular.
- Consumo eléctrico.
- Videovigilancia.
- Inspecciones.
- Decomisos.
- Incidentes anteriores.

RD Propone RD Propone

La coincidencia temporal de varios indicadores podrá servir para priorizar una inspección. Ninguno deberá utilizarse aisladamente como prueba automática de responsabilidad.

30. Sistema de puntuación de riesgo

Podrá desarrollarse un modelo técnico interno que asigne niveles de riesgo a determinadas zonas. Por ejemplo:

- Detección recurrente de señal.
- Hallazgo previo de cargadores.
- Manipulación eléctrica.
- Incidentes anteriores.
- Consumo anormal.

El resultado servirá exclusivamente para orientar recursos de inspección y prevención.

31. Auditoría eléctrica penitenciaria

Los establecimientos deberán realizar auditorías periódicas de seguridad eléctrica. Estas deberán diferenciarse de las inspecciones tradicionales destinadas únicamente a determinar si una instalación funciona correctamente. Estas responderán:

- ¿Puede accederse fácilmente al tomacorriente?
- ¿Puede manipularse?
- ¿Puede utilizarse un circuito para cargar equipos clandestinos?
- ¿Existen conexiones improvisadas?
- ¿Existen zonas sin control?
- ¿Se han alterado sellos?
- ¿Coinciden los planos con la instalación real?

32. Certificación periódica

Los centros podrán someterse a un procedimiento de certificación de seguridad eléctrica penitenciaria. La certificación comprobará:

- Integridad de instalaciones.
- Protección contra manipulación.
- Separación de circuitos.
- Control de accesos eléctricos.
- Funcionamiento de sistemas de monitoreo.

RD Propone RD Propone

- Corrección de vulnerabilidades.

La certificación deberá renovarse periódicamente.

33. Intervención ante manipulación

Cuando se detecte una modificación no autorizada deberán realizarse simultáneamente dos acciones.

Primero, restablecer inmediatamente la seguridad eléctrica. Segundo, investigar el origen de la modificación.

Debe determinarse cómo, cuándo y eventualmente con qué materiales fue realizada la alteración.

34. Investigación de materiales utilizados

Los componentes encontrados en conexiones clandestinas deberán registrarse. Esto podrá permitir identificar:

- Procedencia.
- Tipo de material.
- Repetición de técnicas.
- Posibles fuentes internas.
- Relacionamiento con trabajos recientes.

La información deberá incorporarse al análisis general de seguridad.

35. Capacitación del personal técnico

Los electricistas y técnicos que trabajen dentro del sistema penitenciario deberán recibir capacitación específica. Además de conocimientos eléctricos deberán reconocer:

- Métodos comunes de manipulación.
- Componentes que pueden utilizarse para obtener energía.
- Señales de alteración.
- Procedimientos de cadena de custodia.
- Protocolos de reporte.

36. Prohibición de improvisaciones institucionales

RD Propone RD Propone

Una práctica informal creada por la propia administración puede convertirse posteriormente en una vulnerabilidad. Toda instalación temporal deberá estar autorizada, documentada y retirada cuando termine su finalidad.

37. Seguridad contra incendios

Todas las medidas contempladas deberán respetar estrictamente las normas de prevención de incendios. La eliminación, protección o administración de tomacorrientes nunca deberá conducir a que las personas recurran a conexiones más peligrosas. Por ello, la política deberá combinar restricciones con inspecciones y mantenimiento preventivo.

38. Protección de servicios esenciales

No podrán utilizarse medidas de control energético que comprometan:

- Iluminación mínima.
- Ventilación.
- Equipos médicos.
- Sistemas de emergencia.
- Bombas de agua.
- Sistemas contra incendios.
- Seguridad electrónica.
- Comunicaciones institucionales.

Servicios indispensables para condiciones dignas de internamiento.

39. Coordinación con organismos técnicos

El diseño de la política eléctrica deberá contar con participación de profesionales de ingeniería eléctrica, seguridad contra incendios, arquitectura penitenciaria y prevención de riesgos.

La autoridad penitenciaria no deberá definir unilateralmente especificaciones eléctricas sin respaldo técnico.

40. Indicadores de desempeño

Se medirán, entre otros:

- Cantidad de tomas vulnerables identificadas.
- Cantidad de conexiones clandestinas encontradas.
- Número de cargadores decomisados.

RD Propone RD Propone

- Cantidad de baterías externas decomisadas.
- Incidentes por manipulación eléctrica.
- Tiempo de reparación.
- Bloques con reincidencias.
- Reducción de puntos de libre acceso.
- Resultados de auditorías.

41. Programa de adecuación nacional

Se elaborará un inventario nacional de vulnerabilidades eléctricas penitenciarias. Los centros serán clasificados por nivel de riesgo.

A partir de esta clasificación se establecerá un programa plurianual de adecuación. Las intervenciones podrán comenzar con medidas relativamente económicas:

- Protección de cajas.
- Retiro de tomas innecesarias.
- Sellos.
- Separación de determinados circuitos.
- Monitoreo básico.

Para posteriormente incorporar soluciones de mayor complejidad.

42. Principio de proporcionalidad económica

No todos los centros requerirán la misma tecnología. Las soluciones deberán guardar relación con:

- Tamaño.
- Cantidad de internos.
- Nivel de riesgo.
- Edad de la infraestructura.
- Historial de incidentes.
- Características constructivas.
- Capacidad presupuestaria.

El objetivo será obtener la mayor reducción de vulnerabilidad posible por cada inversión realizada.

43. Resultado esperado

RD Propone RD Propone

La finalidad será que un dispositivo clandestino que haya logrado ingresar a un centro penitenciario encuentre dificultades adicionales para mantenerse operativo.

La persona que pretenda utilizarlo deberá enfrentar no solamente controles de ingreso y restricciones de telecomunicaciones, sino también:

Escasez de puntos de carga accesibles / Imposibilidad de manipular fácilmente instalaciones / Control de cargadores y cables / Control de baterías / Monitoreo de circuitos / Inspecciones técnicas / Trazabilidad de alteraciones.

La energía eléctrica pasará así de ser una vulnerabilidad pasiva a convertirse en una capa activa de seguridad penitenciaria. El objetivo no será privar de electricidad a las personas privadas de libertad. Será impedir que la infraestructura eléctrica legítima del Estado se convierta, sin control, en el recurso que permita mantener operativas comunicaciones clandestinas utilizadas para la comisión de delitos.

CAPÍTULO VI
VIDEOVIGILANCIA INTELIGENTE, ELIMINACIÓN DE PUNTOS CIEGOS Y TRAZABILIDAD DE MOVIMIENTOS

1. Objeto del capítulo

El presente capítulo establece los lineamientos para desarrollar un Sistema Integral de Videovigilancia Penitenciaria destinado a prevenir, detectar e investigar la introducción, traslado, ocultamiento, intercambio y utilización de dispositivos tecnológicos no autorizados dentro de los centros penitenciarios.

La videovigilancia deberá funcionar como una herramienta integrada con los demás componentes del sistema de seguridad y no como un mecanismo aislado.

Su finalidad será permitir que los movimientos relacionados con dispositivos clandestinos puedan ser reconstruidos y analizados cuando exista una alerta, decomiso o incidente de seguridad.

2. Principio de cobertura estratégica

La política no deberá perseguir simplemente instalar la mayor cantidad posible de cámaras.

El objetivo será conseguir *cobertura estratégica, continua y verificable de las rutas y áreas donde exista mayor riesgo de introducción, transferencia u ocultamiento de objetos prohibidos.*

RD Propone RD Propone

Cada cámara deberá responder a una necesidad concreta de seguridad.

3. Mapa nacional de videovigilancia penitenciaria

Cada centro deberá elaborar un mapa actualizado de videovigilancia. Este deberá identificar:

a) Ubicación de cámaras;

b) Área cubierta;

c) Ángulo aproximado de observación;

d) Zonas sin cobertura;

e) Cámaras fuera de servicio;

f) Áreas de especial sensibilidad;

g) Rutas de circulación;

h) Accesos y salidas;

i) Zonas de transferencia de mercancías;

j) Áreas de almacenamiento.

El mapa deberá utilizarse para identificar y eliminar progresivamente puntos ciegos.

4. Eliminación de puntos ciegos

Los centros deberán realizar inspecciones periódicas destinadas específicamente a localizar puntos que permitan actividades fuera del alcance razonable de los sistemas de vigilancia. Se prestará especial atención a:

1. Escaleras.
2. Pasillos.
3. Intersecciones.
4. Puertas secundarias.
5. Áreas detrás de edificaciones.
6. Patios.
7. Zonas de almacenamiento.
8. Muelles de carga.
9. Áreas próximas a muros.

RD Propone RD Propone

10. Espacios de transferencia de mercancías.

Los puntos ciegos detectados deberán clasificarse según nivel de riesgo y corregirse progresivamente.

5. Cobertura de accesos

Todos los accesos principales deberán estar sometidos a videovigilancia. Esto comprenderá:

a) Entrada de visitantes;

b) Entrada del personal;

c) Entrada de contratistas;

d) Entrada de proveedores;

e) Accesos vehiculares;

f) Recepción de paquetes;

g) Recepción de mercancías;

h) Salidas correspondientes.

La grabación deberá permitir reconstruir posteriormente quién ingresó, cuándo lo hizo y por cuál punto.

6. Videovigilancia del personal

Las rutas utilizadas habitualmente por empleados y agentes deberán encontrarse bajo cobertura adecuada.

El objetivo no será presumir irregularidades del personal, sino garantizar que ninguna categoría de persona disponga de corredores completamente ajenos a los sistemas de seguridad. Los controles deberán aplicarse mediante criterios institucionales y generales.

7. Mercancías bajo trazabilidad visual

Las áreas donde se reciben alimentos, medicamentos, materiales de construcción, ropa, herramientas y demás bienes deberán estar cubiertas por cámaras.

La política procurará que pueda reconstruirse visualmente el recorrido de una mercancía desde su recepción hasta su entrega en la zona correspondiente.

RD Propone RD Propone

Especial atención deberá prestarse a los puntos donde una carga cambia de responsable.

8. Zonas de transferencia

Toda zona donde objetos pasen del exterior al interior deberá considerarse área crítica. Estas zonas deberán contar con cobertura suficiente para observar:

1. Recepción.
2. Inspección.
3. Apertura.
4. Clasificación.
5. Transferencia.
6. Retiro.

El sistema deberá procurar que ninguna entrega desaparezca visualmente durante etapas críticas del proceso.

9. Talleres y trabajos de mantenimiento

Los trabajos de construcción, reparación, electricidad, telecomunicaciones y mantenimiento pueden generar circunstancias particulares de riesgo.

Las áreas intervenidas deberán recibir vigilancia adicional cuando resulte necesario.

Asimismo, deberá registrarse visualmente la entrada y salida de herramientas y materiales cuando la naturaleza del trabajo lo justifique.

10. Perímetro exterior

La seguridad deberá extenderse al perímetro. Las cámaras podrán utilizarse para identificar:

1. Movimientos próximos a muros.
2. Lanzamientos de objetos.
3. Vehículos detenidos en lugares inusuales.
4. Actividad nocturna.
5. Posibles operaciones con drones.
6. Intentos de acercamiento a zonas restringidas.

La cobertura deberá diseñarse de acuerdo con las características geográficas de cada establecimiento.

RD Propone RD Propone

11. Áreas de visitas

Las áreas generales de acceso y circulación relacionadas con visitas podrán contar con videovigilancia. Deberán diferenciarse claramente de espacios donde puedan producirse comunicaciones legalmente protegidas o situaciones que requieran especial privacidad.

La vigilancia deberá diseñarse atendiendo al principio de proporcionalidad.

12. Protección de espacios de intimidad

No deberán instalarse cámaras de manera que impliquen vigilancia indiscriminada en espacios donde exista una expectativa particularmente elevada de privacidad. Deberán establecerse restricciones específicas para:

a) Baños;

b) Duchas;

c) Áreas médicas destinadas a consultas privadas;

d) Espacios de comunicación confidencial con abogados;

e) Otros espacios cuya vigilancia permanente resulte incompatible con derechos fundamentales.

Cuando razones extraordinarias de seguridad exijan medidas especiales, estas deberán disponer de fundamento jurídico, supervisión y límites definidos.

13. Cámaras resistentes a manipulación

Los equipos instalados dentro de zonas penitenciarias deberán utilizar diseños apropiados para entornos de alta seguridad. Se procurará incorporar:

- Protección física.
- Carcasas resistentes.
- Cableado protegido.
- Instalación fuera del alcance directo cuando sea posible.
- Alertas por desconexión.
- Alertas por pérdida de imagen.
- Protección contra alteraciones.

14. Detección de obstrucción

RD Propone RD Propone

Los sistemas deberán identificar, cuando resulte técnicamente viable, situaciones en las cuales una cámara sea:

- Tapada.
- Girada.
- Desconectada.
- Desenfocada deliberadamente.
- Cubierta parcialmente.
- Bloqueada mediante algún objeto.

La alteración deberá generar una alerta.

15. Supervisión del estado de cámaras

El Centro Nacional de Monitoreo deberá poder conocer cuáles cámaras se encuentran operativas. Una cámara fuera de servicio durante períodos prolongados deberá generar incidencias de mantenimiento. El sistema deberá registrar:

1. Hora de falla.
2. Duración.
3. Motivo.
4. Hora de reparación.
5. Técnico responsable.

16. Grabación continua

Las zonas críticas deberán disponer preferentemente de grabación continua. El período de conservación deberá establecerse mediante normas específicas tomando en consideración:

1. Capacidad tecnológica.
2. Necesidades de investigación.
3. Protección de datos.
4. Costos.
5. Naturaleza de cada área.

Cuando una grabación esté relacionada con un incidente, deberá conservarse durante el tiempo necesario para las investigaciones correspondientes.

17. Marcación automática de incidentes

RD Propone RD Propone

Una de las funciones más importantes será integrar las cámaras con otras fuentes de alerta.

Cuando el sistema detecte actividad celular sospechosa en una zona determinada, podrá marcar automáticamente las grabaciones relacionadas. Por ejemplo:

Alerta tecnológica: Bloque C 22:13 a 22:27

El sistema deberá permitir recuperar rápidamente las cámaras correspondientes a dicho bloque y período.

18. Integración con alertas eléctricas

El mismo procedimiento podrá aplicarse cuando exista una alerta relacionada con consumo eléctrico anormal. Podrá elevar el nivel de atención sobre determinada zona, la coincidencia entre:

1. Actividad celular.
2. Consumo eléctrico atípico.
3. Movimiento observado.
4. Antecedentes de decomisos.

19. Línea temporal integrada

Los centros deberán avanzar hacia sistemas que permitan observar diferentes eventos sobre una misma línea temporal. Por ejemplo:

21:52: ingreso de funcionario.

22:04: apertura de determinada área.

22:17: actividad celular detectada.

22:19: consumo eléctrico anormal.

22:27: cesa la señal.

22:32: movimiento registrado en corredor.

La coincidencia de eventos servirá para orientar investigaciones. No constituirá por sí sola prueba automática de responsabilidad.

20. Analítica de video

RD Propone RD Propone

Podrán incorporarse herramientas tecnológicas capaces de identificar situaciones que requieran revisión humana. Estas podrían ayudar a detectar:

1. Acceso a áreas restringidas.
2. Movimientos durante horarios inusuales.
3. Permanencia prolongada en zonas determinadas.
4. Manipulación de determinados espacios.
5. Objetos abandonados.
6. Concentraciones inusuales.

Las alertas deberán ser verificadas por personal capacitado.

21. Prohibición de decisiones disciplinarias automáticas

Ningún algoritmo o sistema de análisis de imágenes deberá imponer por sí mismo una sanción. La tecnología podrá generar alertas o identificar eventos.

Toda determinación de responsabilidad deberá realizarse mediante los procedimientos administrativos, disciplinarios o judiciales correspondientes.

22. Uso de reconocimiento facial

Cualquier eventual utilización de tecnologías de reconocimiento facial deberá someterse previamente a evaluación jurídica, técnica y de protección de datos. No deberá incorporarse automáticamente por el simple hecho de encontrarse disponible comercialmente.

23. Trazabilidad de movimientos autorizados

Cuando resulte operacionalmente apropiado, el registro electrónico de acceso podrá complementarse con la videovigilancia. Esto permitiría determinar si una persona:

1. Ingresó.
2. Pasó por determinadas zonas.
3. Accedió a un área autorizada.
4. Permaneció durante determinado período.
5. Salió.

El objetivo será reconstruir hechos cuando ocurra un incidente.

24. Credenciales electrónicas

RD Propone RD Propone

El personal podrá utilizar credenciales de acceso individualizadas. Las puertas electrónicas podrán registrar:

1. Usuario.
2. Hora.
3. Puerta.
4. Entrada.
5. Salida.

El sistema podrá cruzar posteriormente esta información con imágenes de seguridad.

25. Prohibición de credenciales compartidas

El préstamo o utilización de credenciales pertenecientes a otra persona deberá estar expresamente prohibido. Cuando existan razones justificadas para accesos excepcionales, deberán registrarse.

26. Control de puertas críticas

Las puertas que comuniquen zonas de distinto nivel de seguridad deberán recibir especial protección. Podrán utilizarse mecanismos como:

- Registro electrónico.
- Cámara asociada.
- Alarma de apertura prolongada.
- Doble autorización en áreas especialmente sensibles.
- Alertas por apertura fuera de horario.

27. Supervisión de almacenes

Los almacenes constituyen espacios relevantes debido a la cantidad de materiales que entran y salen. Deberán existir controles sobre:

1. Personas que ingresan.
2. Hora.
3. Material retirado.
4. Material entregado.
5. Duración de permanencia.

28. Cocinas y áreas de alimentos

RD Propone RD Propone

Debido al volumen de mercancías y movimiento de personas, las cocinas y áreas de recepción de alimentos deberán incluirse dentro del mapa de riesgos.

Los controles deberán diseñarse sin interferir innecesariamente con las actividades ordinarias del servicio.

29. Seguimiento posterior a decomisos

Cuando se encuentre un teléfono o dispositivo prohibido, la investigación deberá revisar las grabaciones relevantes. El análisis buscará determinar:

- Cómo pudo llegar al área.
- Quiénes tuvieron acceso.
- Si fue trasladado.
- Cuándo apareció por primera vez.
- Qué rutas pudieron utilizarse.

Esto permitirá convertir el decomiso en información preventiva.

30. Reconstrucción de rutas

El sistema deberá permitir reconstruir secuencias razonables de movimiento. Por ejemplo:

Entrada de mercancía / Almacén / Traslado interno / Bloque / Area donde aparece el dispositivo.

Cuando una misma ruta aparezca repetidamente asociada a decomisos, deberá clasificarse como vulnerabilidad prioritaria.

31. Mapa de calor de incidentes

Los datos de cámaras, decomisos y alertas podrán utilizarse para crear mapas internos de concentración de incidentes. Estos mostrarán visualmente:

1. Áreas de mayor frecuencia.
2. Horarios.
3. Días.
4. Rutas.
5. Tipos de incidentes.

El objetivo será identificar patrones que no resulten evidentes mediante observación individual.

RD Propone RD Propone

32. Protección de grabaciones

Las grabaciones deberán almacenarse mediante sistemas que reduzcan la posibilidad de:

1. Eliminación no autorizada.
2. Edición.
3. Sustitución.
4. Acceso indebido.
5. Copia clandestina.

El sistema deberá registrar quién accede a determinadas grabaciones.

33. Registro de accesos a videos

Toda consulta de grabaciones relacionadas con investigaciones deberá dejar trazabilidad. Deberá registrarse:

- Usuario.
- Fecha.
- Hora.
- Grabación consultada.
- Motivo.
- Descarga realizada, si corresponde.

Esto permitirá auditar posibles usos indebidos.

34. Exportación de evidencia

Cuando una grabación deba utilizarse en una investigación administrativa o penal, deberá existir un procedimiento que preserve su autenticidad. Se deberán establecer mecanismos de:

- Identificación.
- Copia segura.
- Sellado digital cuando resulte posible.
- Registro.
- Cadena de custodia.
- Entrega a autoridad competente.

35. Centro local de monitoreo

RD Propone RD Propone

Los establecimientos de mayor tamaño deberán contar con capacidades locales de monitoreo. El personal deberá recibir capacitación específica y trabajar bajo protocolos.

La existencia de cámaras no tendrá utilidad si nadie revisa alertas ni existe capacidad para responder.

36. Supervisión nacional

Determinados eventos de alto nivel podrán ser visualizados o reportados al Centro Nacional de Monitoreo Penitenciario. Esto permitirá:

1. Supervisión.
2. Asistencia técnica.
3. Detección de patrones nacionales.
4. Verificación de fallas.
5. Coordinación en incidentes graves.

37. Separación de funciones

Cuando sea posible, las personas responsables de supervisar determinadas grabaciones no deberán ser las únicas con capacidad para eliminarlas o modificar configuraciones.

La separación de funciones reducirá riesgos de encubrimiento.

38. Auditorías sorpresa de cámaras

Las auditorías periódicas deberán verificar:

- Cobertura.
- Calidad de imagen.
- Grabación.
- Fecha y hora correctas.
- Almacenamiento.
- Alertas.
- Acceso.
- Mantenimiento.
- Puntos ciegos.

Se deberán realizar pruebas reales y no limitarse a verificar que los equipos estén instalados.

39. Indicador de disponibilidad

RD Propone RD Propone

Una elevada cantidad de cámaras inoperativas deberá generar intervención administrativa y técnica. Los indicadores deberán distinguir entre:

1. Fallas programadas.
2. Mantenimiento.
3. Fallas inesperadas.
4. Manipulación.
5. Daños.

40. Protección contra corrupción interna

La videovigilancia deberá contribuir también a detectar posibles redes internas de introducción de dispositivos, sin embargo, ninguna persona deberá ser investigada exclusivamente por su presencia en una grabación.

Las imágenes deberán analizarse conjuntamente con otros elementos objetivos.

41. Canal de denuncia

La política podrá incorporar mecanismos confidenciales para que empleados, internos, familiares o terceros comuniquen información sobre rutas de introducción de teléfonos.

Las denuncias deberán ser evaluadas antes de generar actuaciones invasivas o acusaciones.

Cuando la información resulte verificable, podrá utilizarse para orientar la revisión de cámaras.

42. Inteligencia acumulativa

Cada incidente deberá incorporarse al sistema de aprendizaje institucional.

Si un nuevo caso demuestra que una zona aparentemente segura fue utilizada para transferir un dispositivo, el mapa de riesgos deberá actualizarse.

La infraestructura de vigilancia deberá adaptarse conforme cambien los métodos de evasión.

43. Inteligencia artificial aplicada a videovigilancia

La incorporación futura de inteligencia artificial deberá utilizarse principalmente como herramienta de apoyo. Podrá facilitar:

- Búsqueda de eventos.

RD Propone RD Propone

- Clasificación de grabaciones.
- Detección de anomalías.
- Identificación de secuencias.
- Correlación temporal.

No deberá sustituir la evaluación humana en decisiones que afecten derechos.

44. Evaluación de precisión

Todo sistema automatizado deberá probarse antes de su uso operativo. La administración deberá conocer:

1. Tasa de falsas alarmas.
2. Tasa de eventos omitidos.
3. Condiciones en que disminuye su precisión.
4. Limitaciones técnicas.

Un sistema que produzca demasiadas alertas incorrectas puede terminar disminuyendo la seguridad en lugar de aumentarla.

45. Capacitación

Los operadores deberán recibir formación sobre:

1. Manejo de cámaras.
2. Protección de datos.
3. Identificación de incidentes.
4. Preservación de evidencia.
5. Cadena de custodia.
6. Derechos fundamentales.
7. Uso de analítica.
8. Procedimientos de respuesta.

46. Mantenimiento preventivo

Los sistemas de videovigilancia deberán disponer de mantenimiento periódico. Los contratos tecnológicos deberán contemplar:

1. Limpieza.
2. Reparación.
3. Reemplazo.

RD Propone RD Propone

4. Actualización.
5. Almacenamiento.
6. Repuestos.
7. Soporte.
8. Tiempo máximo de respuesta.

47. Contratación basada en resultados

Los procesos de adquisición deberán evaluar más que la cantidad de cámaras, deberán considerar:

1. Cobertura.
2. Resolución apropiada.
3. Disponibilidad.
4. Capacidad nocturna.
5. Integración.
6. Almacenamiento.
7. Ciberseguridad.
8. Resistencia.
9. Interoperabilidad.
10. Costo total de mantenimiento.

48. Indicadores de desempeño

El sistema deberá medir:

- Cantidad de cámaras instaladas.
- Porcentaje operativo.
- Puntos ciegos identificados.
- Puntos ciegos corregidos.
- Incidentes detectados mediante cámaras.
- Decomisos apoyados por videovigilancia.
- Tiempo de recuperación de grabaciones.
- Intentos de manipulación.
- Fallas recurrentes.
- Investigaciones apoyadas por imágenes.

49. Evaluación anual

RD Propone RD Propone

Cada centro deberá realizar una evaluación anual de su sistema. Esta deberá determinar:

1. Qué funcionó.
2. Qué zonas continúan vulnerables.
3. Qué cámaras deben reubicarse.
4. Qué tecnologías necesitan actualización.
5. Qué patrones nuevos se identificaron.

La videovigilancia deberá evolucionar junto con las amenazas.

50. Resultado esperado

La finalidad será conseguir que los principales movimientos de personas, mercancías y objetos dentro de las áreas críticas de un centro penitenciario puedan ser reconstruidos razonablemente cuando ocurra un incidente.

Una persona que pretenda introducir, transportar o entregar clandestinamente un dispositivo deberá enfrentar:

Controles de entrada / Registro de acceso / Cámaras / Trazabilidad de rutas / Alertas tecnológicas / Correlación temporal / Revisión posterior / Investigación del decomiso.

El propósito no será convertir el centro penitenciario en un espacio de vigilancia indiscriminada.

Será asegurar que las rutas críticas de seguridad estén suficientemente controladas para dificultar el movimiento clandestino de dispositivos y facilitar la identificación de vulnerabilidades, redes de introducción y posibles complicidades.

CAPÍTULO VII
INTEGRIDAD DEL PERSONAL, CORRUPCIÓN, COMPLICIDAD INTERNA Y RÉGIMEN DE RESPONSABILIDADES

1. Objeto del capítulo

El presente capítulo establece los lineamientos destinados a prevenir, detectar, investigar y sancionar la participación de funcionarios, agentes penitenciarios, contratistas, suplidores, visitantes u otras personas en la introducción, facilitación, ocultamiento, utilización o protección de dispositivos tecnológicos no autorizados dentro de los centros penitenciarios.

RD Propone RD Propone

La política reconoce que la seguridad penitenciaria no depende únicamente de infraestructura, cámaras, bloqueadores, detectores o controles eléctricos.

Cualquier sistema puede resultar debilitado si una persona con acceso legítimo utiliza deliberadamente sus funciones para facilitar actividades prohibidas.

Por esta razón, la integridad institucional deberá constituir una capa independiente de seguridad.

2. Principio de responsabilidad diferenciada

Las responsabilidades deberán determinarse tomando en consideración la condición y función de cada persona involucrada. La política distinguirá entre:

a) Persona privada de libertad que posea o utilice un dispositivo no autorizado;

b) Visitante que intente introducirlo;

c) Contratista o proveedor que participe deliberadamente;

d) Funcionario o agente que facilite su ingreso;

e) Funcionario que omita deliberadamente controles;

f) Persona que participe a cambio de dinero, favores u otros beneficios;

g) Persona que forme parte de una estructura organizada destinada a introducir dispositivos;

h) Persona que facilite comunicaciones destinadas a la comisión de otros delitos.

La respuesta jurídica deberá ser proporcional a la gravedad y circunstancias de cada conducta.

3. Deber reforzado del personal penitenciario

Los funcionarios y agentes encargados de la custodia, administración o seguridad de centros penitenciarios tienen un deber especial de protección del sistema. En consecuencia, la participación deliberada de un servidor penitenciario en la introducción o facilitación de teléfonos, tarjetas SIM, cargadores, baterías o dispositivos similares deberá considerarse particularmente grave.

Esta valoración responde a que el servidor no solamente participa en una conducta prohibida, sino que aprovecha una posición de confianza y acceso institucional.

RD Propone RD Propone

4. Evaluación de agravamiento normativo

La política deberá realizar una revisión completa del régimen penal, administrativo y disciplinario vigente para determinar si las sanciones actuales resultan suficientes.

Cuando se identifiquen vacíos normativos, podrá proponerse un régimen agravado cuando la conducta sea realizada por:

a) Funcionarios penitenciarios;

b) Personal de seguridad;

c) Servidores públicos;

d) Contratistas con acceso privilegiado;

e) Personas que actúen como parte de una organización criminal.

Cualquier reforma deberá respetar los principios constitucionales de legalidad, proporcionalidad, culpabilidad, debido proceso y derecho de defensa.

5. Destitución e inhabilitación

Cuando exista condena o decisión administrativa firme conforme al procedimiento correspondiente, podrá evaluarse la aplicación de consecuencias adicionales para funcionarios responsables.

Estas podrán comprender, según la gravedad y el marco legal aplicable:

- Destitución.
- Separación del servicio.
- Inhabilitación temporal para ocupar determinadas funciones penitenciarias.
- Prohibición de acceso futuro a zonas restringidas.
- Registro institucional del incidente.

Estas consecuencias no deberán aplicarse automáticamente sin procedimiento previo.

6. Responsabilidad penal independiente

La responsabilidad disciplinaria no deberá sustituir la responsabilidad penal cuando los hechos constituyan delitos.

RD Propone RD Propone

Cuando existan indicios suficientes de corrupción, soborno, asociación delictiva, tráfico de objetos prohibidos, extorsión, complicidad u otras infracciones, la información deberá remitirse al Ministerio Público.

El nuevo Código Penal dominicano contempla la corrupción pública como conducta asociada al aprovechamiento de la función pública para beneficios o actividades ilícitas.

7. Prohibición expresa de introducción y facilitación

La normativa interna deberá establecer de forma expresa que ningún funcionario, contratista, suplidor o visitante podrá:

a) Introducir dispositivos no autorizados;

b) Transportarlos dentro del establecimiento;

c) Entregarlos a personas privadas de libertad;

d) Facilitar cargadores, baterías o SIM;

e) Permitir deliberadamente su ingreso;

f) Desactivar controles para facilitarlo;

g) Alterar registros;

h) Ocultar decomisos;

i) Manipular cámaras o sistemas tecnológicos para evitar detección;

j) Advertir previamente sobre requisas u operativos confidenciales.

8. Control equivalente para personal y visitantes

Los funcionarios no deberán quedar automáticamente exentos de controles.

La política establecerá mecanismos de inspección apropiados y proporcionales para el personal. Estos podrán incluir:

- Control de dispositivos personales.
- Casilleros externos.
- Detectores.
- Revisión aleatoria.
- Registro de equipos autorizados.
- Controles de salida.

RD Propone RD Propone

La aplicación deberá hacerse mediante criterios uniformes y no discriminatorios.

9. Casilleros exteriores obligatorios

Los teléfonos personales del personal que no requieran autorización institucional deberán permanecer fuera de las áreas restringidas. Los establecimientos deberán disponer de casilleros seguros. El sistema podrá registrar:

- Funcionario.
- Número de casillero.
- Hora de depósito.
- Hora de retiro.

Esto reducirá significativamente la cantidad de teléfonos legítimos presentes dentro del establecimiento.

10. Dispositivos institucionales diferenciados

Cuando determinado personal necesite teléfono móvil para su función, deberá utilizar preferentemente equipos institucionales. Estos deberán estar registrados y claramente identificados. El sistema deberá permitir diferenciar un dispositivo oficial de uno particular.

11. Inspecciones aleatorias del personal

Podrán realizarse controles aleatorios de entrada o salida conforme a procedimientos previamente establecidos. La selección deberá ser verdaderamente aleatoria cuando esa sea la modalidad declarada.

Se deberá evitar que una misma autoridad pueda elegir discrecionalmente a quién inspeccionar sin criterios verificables.

12. Control al finalizar turno

Determinadas áreas de alto riesgo podrán implementar verificaciones de salida. El objetivo será detectar no solamente objetos introducidos, sino también:

- SIM decomisadas informalmente.
- Teléfonos retirados del inventario.
- Componentes tecnológicos.
- Evidencias.
- Otros objetos institucionales.

RD Propone RD Propone

13. Separación de funciones

Ninguna persona debería controlar por sí sola todas las etapas de un procedimiento crítico. Por ejemplo, siempre que resulte operativamente posible, deberán separarse funciones como:

- Recepción de mercancías.
- Autorización de ingreso.
- Inspección.
- Entrega interna.
- Registro.
- Supervisión.

Esta separación disminuye oportunidades de corrupción.

14. Doble validación en operaciones excepcionales

Determinadas excepciones deberán requerir autorización de más de una persona. Por ejemplo:

- Ingreso extraordinario de equipos tecnológicos.
- Ingreso de mercancías fuera de horario.
- Acceso a zonas particularmente sensibles.
- Desactivación temporal de controles.

Toda excepción deberá quedar registrada.

15. Rotación en posiciones sensibles

Los puestos particularmente expuestos a riesgos de corrupción podrán estar sujetos a políticas razonables de rotación. La rotación podrá aplicarse, entre otros, a:

- Puntos de acceso.
- Recepción de mercancías.
- Almacenes.
- Áreas de visitas.
- Control de cámaras.
- Inventarios tecnológicos.

La rotación no deberá ser arbitraria ni perjudicar injustificadamente la especialización del personal.

RD Propone RD Propone

16. Evaluación de vulnerabilidad de puestos

La administración deberá identificar posiciones con mayor capacidad para vulnerar controles. La clasificación deberá considerar:

- Nivel de acceso.
- Frecuencia de contacto con internos.
- Control de mercancías.
- Control de tecnología.
- Posibilidad de autorizar excepciones.
- Capacidad de modificar registros.

La finalidad será establecer controles preventivos proporcionales.

17. Declaración de conflictos de interés

El personal deberá informar situaciones que puedan generar riesgos especiales. Por ejemplo:

1. Relaciones familiares con personas privadas de libertad.
2. Vínculos económicos relevantes con proveedores.
3. Relaciones que comprometan su imparcialidad.

El mecanismo deberá respetar la privacidad y limitarse a información realmente necesaria para seguridad e integridad institucional.

18. Capacitación anticorrupción

Todo el personal deberá recibir formación periódica sobre:

1. Prohibiciones.
2. Responsabilidades.
3. Métodos de captación utilizados por redes criminales.
4. Soborno.
5. Extorsión.
6. Amenazas.
7. Conflictos de interés.
8. Protección al denunciante.
9. Consecuencias disciplinarias y penales.

La capacitación deberá actualizarse a partir de incidentes reales.

RD Propone RD Propone

19. Riesgo de coerción al personal

La política deberá reconocer que un funcionario puede ser objeto de amenazas o extorsión. Por ello, deberá existir un mecanismo confidencial para que pueda informar intentos de presión sin esperar a que se concrete una conducta ilícita.

La institución deberá evaluar medidas de protección cuando exista riesgo real.

20. Canal confidencial de denuncia

Se establecerá un canal nacional para reportar irregularidades relacionadas con dispositivos clandestinos. Podrán denunciar:

1. Funcionarios.
2. Internos.
3. Familiares.
4. Contratistas.
5. Visitantes.
6. Terceros.

Las denuncias podrán recibirse por medios digitales, telefónicos u otros mecanismos seguros.

21. Protección del denunciante

La persona que reporte de buena fe una posible irregularidad deberá estar protegida frente a represalias conforme al marco jurídico aplicable. La identidad del denunciante deberá limitarse al personal estrictamente necesario.

Las denuncias falsas deliberadas deberán diferenciarse de aquellas que, formuladas de buena fe, finalmente no puedan comprobarse.

22. Unidad especializada de integridad penitenciaria

Podrá establecerse una unidad especializada destinada a analizar posibles casos de corrupción o complicidad interna. Esta unidad deberá contar con independencia operacional suficiente respecto de los centros investigados. Sus funciones podrán comprender:

1. Análisis de incidentes.
2. Cruce de información.
3. Investigaciones administrativas.

RD Propone RD Propone

4. Coordinación con el Ministerio Público.
5. Auditorías.
6. Recomendaciones preventivas.

23. Análisis de patrones del personal

El sistema podrá identificar coincidencias estadísticas relevantes. Por ejemplo:

1. Decomisos recurrentes durante determinados turnos.
2. Aumento de incidentes en una puerta específica.
3. Mercancías vinculadas repetidamente a irregularidades.
4. Desactivaciones frecuentes de cámaras.
5. Excepciones autorizadas de manera inusual.

Estos patrones deberán considerarse señales para investigar y no prueba de responsabilidad.

24. Prohibición de culpabilidad algorítmica

Ningún funcionario podrá ser sancionado únicamente porque un sistema informático le asigne un nivel de riesgo. Las herramientas analíticas podrán orientar auditorías o investigaciones.

Toda responsabilidad deberá establecerse mediante evidencia y procedimiento adecuado.

25. Registro de excepciones

Toda decisión que permita saltarse temporalmente un control normal deberá quedar documentada. El registro deberá incluir:

- Funcionario autorizante.
- Motivo.
- Persona beneficiada.
- Fecha.
- Hora.
- Duración.
- Centro.
- Área.

Las excepciones recurrentes deberán ser auditadas.

RD Propone RD Propone

26. Auditoría de accesos administrativos

Los sistemas informáticos deberán registrar cuándo un funcionario:

1. Modifica una lista blanca.
2. Autoriza un teléfono.
3. Desactiva una alerta.
4. Elimina un registro.
5. Accede a una grabación.
6. Modifica una configuración.
7. Autoriza una excepción.

Esto permitirá reconstruir acciones administrativas.

27. Prohibición de eliminación unilateral de evidencia

Ningún funcionario individual deberá disponer de capacidad para eliminar definitivamente por sí solo:

1. Grabaciones vinculadas a incidentes.
2. Registros de decomisos.
3. Alertas.
4. Datos técnicos.
5. Reportes de auditoría.

Cuando la eliminación sea legítima por vencimiento de conservación deberá ejecutarse conforme a reglas automáticas o procedimientos auditables.

28. Control sobre decomisos

Todo dispositivo decomisado deberá ingresar inmediatamente al registro correspondiente. Se prohibirá:

- Retenerlo informalmente.
- Utilizarlo.
- Retirar SIM sin documentar.
- Entregarlo a terceros.
- Destruirlo sin autorización.

Toda evidencia deberá mantenerse bajo cadena de custodia cuando corresponda.

29. Inventarios sorpresa

RD Propone RD Propone

Podrán realizarse auditorías físicas no anunciadas sobre:

- Dispositivos decomisados.
- Equipos institucionales.
- SIM.
- Cargadores.
- Radios.
- Equipos tecnológicos.
- Material almacenado.

Las diferencias deberán investigarse.

30. Investigación de enriquecimiento o beneficios indebidos

Cuando una investigación formal produzca indicios objetivos de que un servidor ha recibido beneficios relacionados con actividades ilícitas, las autoridades competentes podrán aplicar los mecanismos legales disponibles. La política no establecerá vigilancia financiera indiscriminada del personal.

Toda actuación deberá ajustarse a la legislación y a las garantías correspondientes.

31. Relación con proveedores

Los contratos relacionados con alimentos, mantenimiento, construcción, transporte u otros servicios deberán incluir cláusulas claras sobre seguridad penitenciaria. Las empresas deberán comprometerse a:

- Capacitar a su personal.
- Cumplir controles.
- Registrar equipos.
- Informar irregularidades.
- Cooperar con investigaciones legítimas.

El incumplimiento grave podrá generar consecuencias contractuales conforme al debido proceso.

32. Responsabilidad de contratistas

Los contratistas tendrán obligaciones equivalentes respecto a la prohibición de introducir dispositivos clandestinos. Cuando un trabajador externo participe deliberadamente, podrán aplicarse:

RD Propone RD Propone

1. Expulsión del establecimiento.
2. Cancelación de credenciales.
3. Comunicación a la empresa.
4. Terminación contractual cuando corresponda.
5. Remisión a autoridades competentes.

33. Registro nacional de exclusiones

Cuando exista decisión firme que determine que una persona utilizó su acceso institucional para introducir objetos prohibidos, podrá evaluarse un registro de exclusión de acceso a centros penitenciarios.

El registro deberá disponer de fundamento legal, período definido y mecanismos de revisión.

34. Responsabilidad de visitantes

La política deberá establecer consecuencias claras para visitantes que intenten introducir dispositivos. Estas podrán incluir, conforme a la legislación:

- Suspensión temporal de visitas.
- Revocación de autorizaciones.
- Remisión a autoridades competentes.
- Medidas administrativas.

La respuesta deberá considerar gravedad, intencionalidad y reincidencia.

35. Diferenciación entre posesión e introducción

La política deberá distinguir jurídicamente entre quien utiliza un dispositivo y quien crea la vía para introducirlo. La introducción organizada puede representar una conducta de mayor gravedad que la mera posesión. Esto será particularmente relevante cuando exista:

1. Pago.
2. Planificación.
3. Reincidencia.
4. Participación de varias personas.
5. Finalidad criminal externa.

36. Dispositivos utilizados para cometer delitos

RD Propone RD Propone

Cuando un teléfono clandestino sea utilizado para coordinar:

1. Extorsiones.
2. Secuestros.
3. Fraudes.
4. Robos.
5. Tráfico de drogas.
6. Amenazas.
7. Asesinatos.

U otras conductas criminales, las autoridades deberán investigar tanto el delito principal como la estructura que permitió mantener la comunicación desde el establecimiento.

37. Investigación de la cadena completa

La investigación no deberá concluir automáticamente al identificar al interno que poseía el teléfono. Deberá procurar determinar:

1. ¿Quién obtuvo el dispositivo?
2. ¿Quién lo introdujo?
3. ¿Quién lo transportó?
4. ¿Quién lo entregó?
5. ¿Quién suministró la SIM?
6. ¿Quién suministró cargadores o baterías?
7. ¿Existió pago?
8. ¿Existió participación de personal?
9. ¿Para qué fue utilizado?

El objetivo será desarticular la ruta, no solamente decomisar el objeto.

38. Cooperación con el Ministerio Público

La Constitución atribuye al Ministerio Público la dirección de la investigación penal y el ejercicio de la acción pública. La autoridad penitenciaria conservará sus competencias administrativas y disciplinarias.

39. Coordinación con el Ministerio de Justicia

La implementación de esta política deberá coordinarse con el Ministerio de Justicia dentro del proceso de reorganización institucional del sistema penitenciario. La Ley 80-

RD Propone RD Propone

25 creó el Ministerio de Justicia y el modelo institucional contempla la coordinación de las políticas penitenciarias y correccionales desde dicha estructura.

40. Debido proceso disciplinario

Toda investigación administrativa deberá respetar:

- Notificación.
- Derecho a conocer la imputación.
- Acceso a los elementos correspondientes.
- Derecho de defensa.
- Imparcialidad.
- Decisión motivada.
- Recursos disponibles.

La lucha contra la corrupción deberá fortalecer la institucionalidad y no debilitarla mediante procedimientos arbitrarios.

41. Presunción de inocencia

La aparición de un dispositivo durante el turno de determinado funcionario no significará automáticamente responsabilidad. Tampoco la coincidencia con una cámara, puerta o ruta será suficiente por sí sola.

Las decisiones deberán apoyarse en evidencia verificable.

42. Matriz de consecuencias

La política deberá desarrollar posteriormente una matriz nacional que relacione:

1. Tipo de conducta.
2. Condición del responsable.
3. Intencionalidad.
4. Reincidencia.
5. Existencia de beneficio económico.
6. Participación de organización.
7. Finalidad del dispositivo.
8. Consecuencias administrativas.
9. Posibles consecuencias penales.

La matriz contribuirá a aplicar criterios uniformes entre establecimientos.

RD Propone RD Propone

43. Publicación de estadísticas agregadas

La autoridad penitenciaria deberá publicar periódicamente estadísticas generales sobre:

1. Dispositivos decomisados.
2. Intentos de introducción.
3. Casos relacionados con visitantes.
4. Casos relacionados con personal.
5. Investigaciones iniciadas.
6. Medidas correctivas.

No deberán divulgarse datos que comprometan investigaciones, seguridad operacional o derechos individuales.

44. Indicadores de integridad institucional

Se medirán, entre otros:

1. Número de intentos de introducción.
2. Casos vinculados a personal.
3. Casos vinculados a proveedores.
4. Denuncias recibidas.
5. Denuncias verificadas.
6. Tiempo promedio de investigación.
7. Reincidencia por punto de acceso.
8. Excepciones administrativas.
9. Resultados de auditorías.

45. Evaluación periódica

Las medidas deberán revisarse anualmente. La evaluación determinará:

- Nuevas modalidades de corrupción.
- Debilidades en controles.
- Puestos especialmente vulnerables.
- Necesidades de capacitación.
- Cambios regulatorios necesarios.
- Resultados de investigaciones anteriores.

46. Cultura institucional

RD Propone RD Propone

La política deberá promover una cultura en la cual impedir la entrada de dispositivos no sea únicamente responsabilidad de los agentes de seguridad. Directores, técnicos, administrativos, proveedores y demás personal deberán comprender que la integridad de los controles constituye una responsabilidad institucional compartida.

47. Incentivo a buenas prácticas

Las políticas de integridad no deberán basarse exclusivamente en sanciones. Podrán reconocerse centros y unidades que demuestren:

- Reducción sostenida de incidentes.
- Cumplimiento de protocolos.
- Buenas auditorías.
- Detección temprana de vulnerabilidades.
- Cooperación institucional.

La finalidad será fomentar cumplimiento real y no únicamente temor al castigo.

48. Principio de cero tolerancia con la complicidad institucional

La política establecerá como principio que la introducción deliberada de dispositivos por servidores públicos es incompatible con las funciones de seguridad penitenciaria.

La expresión cero tolerancia no significará ausencia de debido proceso.

Significará que todo indicio razonable deberá ser investigado y que ninguna conducta comprobada deberá ignorarse por posición, rango o relación institucional.

49. Resultado esperado

El objetivo será reducir significativamente la posibilidad de que cualquier persona con acceso legítimo se convierta en una vía segura para introducir dispositivos clandestinos.

Quien intente utilizar su posición para vulnerar el sistema deberá enfrentar:

Controles de acceso / Trazabilidad / Cámaras / Auditorías / Separación de funciones / Registros electrónicos / Análisis de patrones / Investigación / Responsabilidad disciplinaria y, cuando corresponda, penal.

La tecnología será útil solamente si quienes administran el sistema están sometidos a controles adecuados y existen consecuencias reales frente a su utilización ilícita.

RD Propone RD Propone

La integridad institucional deberá ser considerada, por tanto, una infraestructura de seguridad tan importante como los muros, cámaras, detectores, sistemas eléctricos y controles de telecomunicaciones.

CAPÍTULO VIII

SISTEMA DE COMUNICACIONES LEGÍTIMAS, SEGURAS Y SUPERVISADAS PARA PERSONAS PRIVADAS DE LIBERTAD

1. Objeto del capítulo

El presente capítulo establece los lineamientos para desarrollar un sistema institucional de comunicaciones legítimas que permita a las personas privadas de libertad mantener contacto razonable con familiares, abogados, autoridades y otras personas autorizadas, sin recurrir a dispositivos clandestinos.

La política parte de un principio fundamental:

La eliminación del teléfono celular ilegal debe estar acompañada por alternativas legítimas, suficientes, accesibles y seguras de comunicación.

La seguridad penitenciaria no deberá confundirse con aislamiento.

2. Principio de sustitución funcional

El sistema deberá procurar que las necesidades legítimas de comunicación puedan satisfacerse mediante canales institucionales. La política buscará reducir progresivamente uno de los incentivos para adquirir teléfonos clandestinos.

Esto no significa equiparar la comunicación penitenciaria con la disponibilidad irrestricta existente fuera del establecimiento, significa ofrecer alternativas razonables, organizadas y compatibles con las exigencias de seguridad.

3. Sistema Nacional de Comunicaciones Penitenciarias

Se desarrollará un Sistema Nacional de Comunicaciones Penitenciarias integrado a la infraestructura de los centros. Este podrá comprender:

a) Telefonía institucional;

RD Propone RD Propone

b) Videollamadas;

c) Salas digitales;

d) Plataformas de comunicación familiar;

e) Sistemas destinados a comunicaciones con abogados;

f) Canales institucionales con organismos públicos;

g) Herramientas tecnológicas para educación y reinserción.

El sistema deberá estar separado, en la medida técnicamente posible, de las redes utilizadas para la administración y seguridad interna.

4. Cuenta individual de comunicación

Cada persona privada de libertad podrá disponer de un perfil institucional de comunicaciones. El perfil podrá contener:

1. Nombre.
2. Número de identificación penitenciaria.
3. Centro.
4. Ubicación administrativa.
5. Personas autorizadas.
6. Relación declarada.
7. Números telefónicos registrados.
8. Historial administrativo de autorizaciones.
9. Restricciones judiciales cuando correspondan.

La existencia de este perfil deberá facilitar la administración sin convertir el sistema en vigilancia indiscriminada de contenidos.

5. Registro de contactos autorizados

Las personas privadas de libertad podrán registrar contactos conforme a procedimientos determinados reglamentariamente. Podrán incluirse:

- Familiares.
- Representantes legales.
- Personas de apoyo autorizadas.
- Representantes consulares cuando corresponda.

RD Propone RD Propone

- Otros contactos legítimos.

Los mecanismos de validación deberán procurar evitar tanto la suplantación como requisitos excesivamente burocráticos.

6. Actualización de contactos

Deberán existir controles para evitar cambios fraudulentos, pero no deberán imponerse restricciones innecesarias que dificulten la comunicación legítima. Los cambios deberán quedar documentados.

7. Telefonía institucional

Los establecimientos deberán disponer progresivamente de sistemas de telefonía institucional destinados a personas privadas de libertad. Los terminales deberán:

1. Ser resistentes.
2. Encontrarse instalados en lugares determinados.
3. Impedir modificaciones no autorizadas.
4. Estar vinculados al sistema penitenciario.
5. Disponer de controles administrativos.

Los equipos no deberán permitir la instalación libre de aplicaciones o componentes.

8. Videollamadas familiares

Podrán establecerse sistemas de videollamadas para facilitar contacto familiar, especialmente cuando:

a) Los familiares residan lejos;

b) Existan dificultades económicas para desplazarse;

c) Haya personas mayores o con discapacidad;

d) Existan familiares en el extranjero;

e) Ocurran situaciones extraordinarias que dificulten visitas presenciales.

La videollamada deberá funcionar como complemento y no necesariamente como sustituto general de las visitas presenciales.

9. Salas digitales

RD Propone RD Propone

Los centros podrán disponer de salas digitales supervisadas. Estas instalaciones podrán utilizarse para:

1. Comunicación familiar.
2. Educación.
3. Procesos de reinserción.
4. Trámites institucionales.
5. Comunicación jurídica.
6. Formación profesional.

El Estado dominicano ya ha iniciado proyectos de este tipo mediante cooperación entre INDOTEL y ONAPREP, por lo que la política deberá evaluar y ampliar progresivamente esa experiencia.

10. Comunicación con abogados

Las comunicaciones entre personas privadas de libertad y sus representantes legales deberán recibir tratamiento diferenciado. La política deberá garantizar la confidencialidad propia de la relación abogado-cliente dentro de los límites establecidos por el ordenamiento jurídico.

Los sistemas destinados a comunicación jurídica no deberán utilizarse para vigilancia indiscriminada de conversaciones protegidas.

11. Cabinas o espacios jurídicos

Los centros podrán disponer de espacios específicos para comunicaciones remotas con abogados. Estos espacios deberán ofrecer:

- Privacidad razonable.
- Identificación del usuario.
- Seguridad física.
- Protección contra utilización por terceros.
- Sistemas institucionales.

El acceso deberá organizarse mediante turnos o citas cuando resulte necesario.

12. Comunicaciones consulares

RD Propone RD Propone

Las personas extranjeras privadas de libertad deberán contar con mecanismos para ejercer los derechos de comunicación consular que les correspondan conforme al marco jurídico aplicable.

El sistema digital podrá facilitar estas comunicaciones cuando resulte apropiado.

13. Comunicaciones con autoridades

Podrán habilitarse canales destinados a comunicación con:

1. Defensoría Pública.
2. Autoridades judiciales.
3. Ministerio Público.
4. Ministerio de Justicia.
5. Organismos de derechos humanos competentes.
6. Otras instituciones conforme correspondan.

La tecnología puede reducir costos y tiempos de traslado para determinados trámites.

14. Tiempo razonable de comunicación

La cantidad de minutos o sesiones podrá variar según:

1. Nivel de seguridad.
2. Situación procesal.
3. Capacidad operativa.
4. Conducta penitenciaria conforme a la ley.
5. Disponibilidad tecnológica.
6. Circunstancias familiares especiales.

Las reglas deberán ser objetivas y transparentes.

15. Prohibición de uso arbitrario como castigo

Las comunicaciones legítimas no deberán ser suspendidas arbitrariamente. Cualquier restricción deberá, contar con fundamento normativo, ser proporcional, tener duración determinada cuando corresponda y ser susceptible de revisión.

Los derechos de defensa y determinadas comunicaciones legalmente protegidas deberán recibir salvaguardas adicionales.

16. Tarifas razonables

RD Propone RD Propone

Cuando determinados servicios impliquen algún costo para el usuario, las tarifas deberán mantenerse bajo criterios de razonabilidad y transparencia. La comunicación familiar no deberá transformarse en una fuente desproporcionada de ingresos.

Los contratos deberán evitar estructuras tarifarias que generen incentivos económicos contrarios al objetivo de reinserción.

17. Personas sin recursos

La política deberá prever mecanismos para que la falta de recursos económicos no produzca aislamiento absoluto. Podrán establecerse cantidades mínimas de comunicación institucional gratuita o subsidiada. Los criterios deberán definirse objetivamente.

18. Horarios de comunicación

Los establecimientos establecerán horarios que permitan compatibilizar:

1. Seguridad.
2. Trabajo penitenciario.
3. Educación.
4. Alimentación.
5. Descanso.
6. Visitas.
7. Actividades institucionales.

El sistema digital podrá utilizar turnos automáticos para reducir conflictos.

19. Reserva de turnos

Cuando la demanda supere la disponibilidad, podrá utilizarse un sistema de reserva. Los turnos podrán asignarse mediante:

1. Orden de solicitud.
2. Rotación.
3. Prioridad por razones justificadas.
4. Situaciones de emergencia familiar.

20. Comunicaciones familiares urgentes

Deberá existir un procedimiento para situaciones extraordinarias. Por ejemplo:

RD Propone RD Propone

- Fallecimiento.
- Enfermedad grave.
- Emergencia familiar.
- Nacimiento.
- Otras circunstancias relevantes.

La administración deberá poder facilitar comunicaciones extraordinarias cuando resulte razonable.

21. Identificación previa

Antes de iniciar determinadas comunicaciones podrá verificarse la identidad de la persona privada de libertad.

Asimismo, cuando resulte necesario, podrán existir mecanismos razonables para validar el contacto externo. El objetivo será impedir la utilización del sistema institucional por personas no autorizadas.

22. Prevención de suplantación

El sistema deberá incorporar medidas para evitar que una persona utilice el perfil asignado a otra. Podrán emplearse:

- Credenciales individuales.
- PIN.
- Tarjetas institucionales.
- Otros sistemas apropiados.

La tecnología biométrica deberá utilizarse únicamente cuando exista fundamento jurídico, necesidad y proporcionalidad.

23. Registro administrativo de llamadas

El sistema podrá registrar datos administrativos tales como:

- Fecha.
- Hora.
- Duración.
- Terminal utilizado.
- Cuenta del interno.
- Número autorizado contactado.

RD Propone RD Propone

Estos registros podrán utilizarse para administración, facturación cuando corresponda y seguridad conforme al marco legal.

24. Diferenciación entre metadatos y contenido

La política deberá distinguir claramente entre datos administrativos de una comunicación y su contenido.

La existencia de sistemas penitenciarios no deberá interpretarse como autorización ilimitada para interceptar o escuchar cualquier conversación.

El acceso al contenido deberá estar sujeto al régimen jurídico correspondiente.

25. Comunicaciones sujetas a supervisión

Cuando determinadas categorías de comunicaciones puedan ser supervisadas legalmente por razones penitenciarias, deberá informarse adecuadamente a los usuarios cuando corresponda. Los procedimientos deberán definir:

- Finalidad.
- Autoridad competente.
- Conservación.
- Acceso.
- Limitaciones.

26. Comunicaciones protegidas

Las comunicaciones que gocen de protección especial conforme a la Constitución o la legislación deberán recibir salvaguardas diferenciadas.

En particular, deberá preservarse adecuadamente la confidencialidad de comunicaciones jurídicas protegidas.

27. Prohibición de comunicaciones delictivas

El acceso a canales legítimos no podrá utilizarse para:

- Amenazas.
- Extorsión.
- Fraude.
- Coordinación criminal.
- Intimidación de víctimas.

RD Propone RD Propone

- Violación de órdenes judiciales.
- Otras actividades ilícitas.

Cuando existan indicios suficientes se aplicarán los procedimientos legales correspondientes.

28. Restricciones individualizadas

Cuando una autoridad competente determine que una persona utiliza los sistemas institucionales para actividades ilícitas, podrán establecerse restricciones específicas conforme al debido proceso.

Siempre que resulte posible, deberán preferirse medidas individualizadas sobre prohibiciones generales.

29. Órdenes judiciales de restricción

El sistema deberá poder ejecutar restricciones judiciales relacionadas con determinados contactos. Por ejemplo, prohibiciones de comunicación con:

- Víctimas.
- Testigos.
- Menores protegidos.
- Personas sujetas a órdenes de alejamiento.
- Otros contactos conforme decisión competente.

30. Lista de contactos restringidos

Cuando exista una orden legal válida, el sistema podrá impedir automáticamente la comunicación con el contacto correspondiente. Toda restricción deberá identificar:

- Autoridad.
- Fecha.
- Fundamento.
- Duración.
- Condiciones de revisión.

31. Protección de víctimas

La creación de canales legítimos de comunicación no deberá generar nuevas oportunidades de intimidación. La política deberá coordinarse con mecanismos de protección de víctimas.

RD Propone RD Propone

Las denuncias de contactos intimidatorios deberán investigarse.

32. Plataforma tecnológica cerrada

Las terminales penitenciarias deberán utilizar preferentemente arquitecturas cerradas. Esto podrá limitar:

- Instalación de aplicaciones.
- Navegación libre.
- Transferencia de archivos no autorizada.
- Cambio de configuración.
- Acceso a redes externas distintas de las permitidas.

33. Dispositivos institucionales

El sistema podrá controlar:

- Aplicaciones instaladas.
- Actualizaciones.
- Permisos.
- Conectividad.
- Usuarios.
- Inventario.

Los dispositivos deberán carecer de funciones no requeridas por los programas autorizados.

34. Educación digital

El mismo ecosistema tecnológico podrá utilizarse para educación. Esto permitirá aprovechar inversiones en infraestructura para:

1. Cursos.
2. Alfabetización digital.
3. Educación formal.
4. Formación técnica.
5. Bibliotecas digitales.
6. Preparación para reinserción.

La política de seguridad no deberá impedir el acceso razonable a tecnología educativa.

35. Alfabetización tecnológica responsable

RD Propone RD Propone

Las personas privadas de libertad podrán recibir capacitación sobre utilización legítima y segura de tecnologías. El objetivo será que la reinserción contemple competencias digitales actuales.

36. Acceso a servicios institucionales

Determinadas terminales podrán permitir solicitudes administrativas. Tales como:

- Citas médicas.
- Solicitudes educativas.
- Trámites internos.
- Consultas de calendario.
- Información institucional.

Esto puede reducir desplazamientos y trámites manuales.

37. Comunicación escrita digital

La política podrá estudiar sistemas institucionales de mensajería escrita. Estos podrán permitir intercambio controlado de mensajes con contactos autorizados. Los mecanismos deberán diseñarse conforme a reglas claras sobre privacidad y seguridad.

38. Prohibición de redes sociales abiertas desde terminales institucionales

Como regla general, los dispositivos destinados a comunicación penitenciaria no deberán proporcionar acceso irrestricto a redes sociales públicas. Cualquier acceso excepcional deberá responder a una finalidad institucional específica.

39. Protección contra contactos indirectos

El diseño deberá evaluar mecanismos utilizados para eludir restricciones. Por ejemplo:

1. Desvío de llamadas.
2. Conferencias no autorizadas.
3. Uso de intermediarios.
4. Reenvíos.
5. Cuentas compartidas.

Las soluciones deberán actualizarse según aparezcan nuevas modalidades.

40. Calidad del servicio

RD Propone RD Propone

La existencia formal de teléfonos institucionales no será suficiente. El sistema deberá medir:

1. Disponibilidad.
2. Tiempo de espera.
3. Calidad.
4. Cantidad de terminales.
5. Fallos.
6. Demanda.
7. Quejas.

Un sistema legítimo que permanentemente esté fuera de servicio puede aumentar el incentivo para recurrir al mercado clandestino.

41. Relación entre población y terminales

Cada centro deberá determinar una proporción adecuada entre población y capacidad de comunicación. Los establecimientos con mayor población requerirán mayor infraestructura.

No deberá aplicarse una cifra uniforme sin considerar las características del centro.

42. Accesibilidad

Los sistemas deberán considerar necesidades de personas con:

1. Discapacidad auditiva.
2. Discapacidad visual.
3. Limitaciones físicas.
4. Dificultades de alfabetización.
5. Barreras lingüísticas.

La accesibilidad formará parte del diseño.

43. Supervisión de proveedores tecnológicos

Cuando los servicios sean prestados mediante empresas externas, los contratos deberán establecer claramente:

- Protección de datos.
- Seguridad.
- Tarifas.

RD Propone RD Propone

- Disponibilidad.
- Mantenimiento.
- Propiedad de información.
- Auditoría.
- Terminación del servicio.
- Interoperabilidad.

44. Protección de datos

Los datos generados deberán estar sometidos a controles apropiados. El acceso se limitará según funciones. La información no deberá utilizarse para fines comerciales ajenos al sistema penitenciario.

45. Ciberseguridad

Los sistemas deberán protegerse contra:

1. Accesos no autorizados.
2. Modificación de perfiles.
3. Robo de credenciales.
4. Manipulación de registros.
5. Instalación de software no autorizado.
6. Extracción de datos.
7. Ataques externos.

Las actualizaciones de seguridad deberán formar parte del mantenimiento ordinario.

46. Auditoría tecnológica

Deberán realizarse pruebas periódicas destinadas a verificar que las terminales institucionales no puedan ser utilizadas fácilmente para eludir las restricciones establecidas. Las vulnerabilidades detectadas deberán corregirse.

47. Integración con la política de celulares clandestinos

El sistema legítimo de comunicación deberá evaluarse conjuntamente con la incidencia de dispositivos ilegales. Será importante conocer si existe relación entre:

1. Disponibilidad de comunicaciones legítimas.
2. Tiempo de espera.
3. Costos.

RD Propone RD Propone

4. Fallos de sistemas.
5. Cantidad de teléfonos clandestinos decomisados.

Esto permitirá comprobar si mejorar el acceso legítimo contribuye a reducir la demanda clandestina.

48. Encuestas periódicas

La administración podrá realizar consultas anónimas sobre funcionamiento del sistema. Podrán participar:

1. Internos.
2. Familiares.
3. Abogados.
4. Personal.

El propósito será identificar problemas operativos. Las encuestas no sustituirán auditorías técnicas.

49. Indicadores nacionales

La política deberá medir, entre otros:

- Cantidad de llamadas legítimas.
- Videollamadas.
- Usuarios.
- Terminales disponibles.
- Disponibilidad del sistema.
- Costo promedio.
- Tiempo de espera.
- Contactos jurídicos.
- Incidentes de utilización indebida.
- Quejas.
- Relación con decomisos clandestinos.

50. Implementación progresiva

El sistema podrá implementarse por etapas. La prioridad deberá asignarse a:

1. Centros con elevada población.
2. Centros con mayor incidencia de teléfonos clandestinos.

RD Propone RD Propone

3. Centros alejados de las principales áreas urbanas.
4. Centros con infraestructura tecnológica disponible.

Las experiencias piloto deberán evaluarse antes de expansión nacional.

51. Evaluación de las salas digitales existentes

Los proyectos de salas digitales ya iniciados en centros penitenciarios deberán ser evaluados. La evaluación deberá determinar:

1. Número de usuarios.
2. Frecuencia de utilización.
3. Capacidad.
4. Seguridad.
5. Impacto educativo.
6. Utilización para comunicaciones familiares.
7. Utilización jurídica.
8. Problemas encontrados.
9. Costos operativos.

Los resultados deberán utilizarse para definir el modelo nacional.

52. Principio de equilibrio

La política deberá mantener un equilibrio permanente entre:

Seguridad pública + Derechos fundamentales + Rehabilitación + Contacto familiar + Integridad institucional.

La eliminación de comunicaciones clandestinas será compatible con la existencia de comunicaciones legítimas organizadas.

53. Resultado esperado

La finalidad será crear un entorno en el cual una persona privada de libertad no necesite recurrir a un teléfono clandestino para mantener comunicaciones legítimas. El sistema deberá ofrecer alternativas controladas que permitan hablar con la familia, comunicarse con abogados, mantener vínculos sociales, realizar determinadas gestiones, acceder a educación digital, sin abrir canales irrestrictos que puedan utilizarse para continuar actividades criminales. La política deberá transmitir una distinción clara, *la comunicación legítima será facilitada; la comunicación clandestina será progresivamente neutralizada.*

RD Propone RD Propone

CAPÍTULO IX
CENTRO NACIONAL DE MONITOREO, INTELIGENCIA Y ANÁLISIS PENITENCIARIO

1. Objeto del capítulo

El presente capítulo establece los lineamientos para la creación de un Centro Nacional de Monitoreo, Inteligencia y Análisis Penitenciario destinado a integrar, procesar y analizar la información generada por los distintos sistemas de seguridad de los centros penitenciarios de la República Dominicana.

El Centro funcionará como instancia nacional de apoyo a la prevención, detección, investigación y respuesta frente a comunicaciones clandestinas, introducción de dispositivos prohibidos, vulnerabilidades tecnológicas, incidentes internos y otras amenazas relacionadas con la seguridad penitenciaria.

Su finalidad no será sustituir la administración ordinaria de cada centro, sino proporcionar una capacidad nacional de supervisión, análisis e inteligencia que permita identificar patrones que difícilmente podrían detectarse mediante el análisis aislado de cada establecimiento.

2. Principio de integración

Los diferentes sistemas tecnológicos no deberán funcionar como plataformas completamente independientes. El Centro deberá procurar integrar progresivamente información proveniente de:

a) Sistemas de detección de dispositivos;

b) Sistemas de control de telecomunicaciones;

c) Videovigilancia;

d) Sistemas eléctricos;

e) Registros de accesos;

f) Decomisos;

g) Inventarios;

h) Registros de visitantes;

i) Controles de proveedores;

RD Propone RD Propone

j) Alertas de seguridad;

k) Auditorías;

l) Investigaciones administrativas.

La integración deberá realizarse respetando las competencias legales de cada institución.

3. Dependencia institucional

El Centro deberá formar parte de la estructura pública responsable de la coordinación y supervisión del sistema penitenciario.

Su adscripción definitiva deberá establecerse conforme a la estructura orgánica del Ministerio de Justicia y de la autoridad penitenciaria correspondiente.

La dirección estratégica deberá permanecer bajo control público.

Las funciones esenciales de inteligencia penitenciaria no deberán ser delegadas íntegramente a empresas privadas.

4. Función principal

La función principal del Centro será transformar grandes cantidades de datos operativos en información útil para la toma de decisiones. No bastará con acumular:

- Videos.
- Alertas.
- Registros.
- Listados.
- Decomisos.
- Reportes.

El sistema deberá relacionarlos para responder preguntas concretas. Por ejemplo:

1. ¿Dónde se detectan más teléfonos?
2. ¿A qué horas?
3. ¿Qué rutas aparecen repetidamente?
4. ¿Qué centros presentan mayor incidencia?
5. ¿Existen dispositivos que reaparecen?
6. ¿Existen patrones asociados con determinadas mercancías?
7. ¿Existen fallas recurrentes en bloqueadores?

RD Propone RD Propone

8. ¿Coinciden determinados eventos tecnológicos con accesos específicos?

5. Tablero nacional

El Centro deberá disponer de un tablero nacional que permita visualizar el estado general del sistema. El tablero podrá mostrar:

- Centros penitenciarios.
- Población.
- Alertas activas.
- Dispositivos detectados.
- Dispositivos decomisados.
- Sistemas fuera de servicio.
- Cámaras inoperativas.
- Alertas eléctricas.
- Incidentes pendientes.
- Nivel de riesgo.
- Resultados de auditorías.

El nivel de detalle disponible dependerá de las credenciales del usuario.

6. Panel individual por centro

Cada establecimiento deberá disponer de un panel específico. Este podrá mostrar:

- Estado de bloqueadores.
- Cobertura.
- Alertas recientes.
- Decomisos.
- Cámaras.
- Incidentes.
- Mantenimiento pendiente.
- Puntos vulnerables.
- Tendencias.

El director del centro podrá utilizar esta información para tomar decisiones operativas.

7. Sala nacional de monitoreo

La sala podrá funcionar permanentemente o mediante esquemas diferenciados según nivel de riesgo. Deberá disponer de:

RD Propone RD Propone

1. Estaciones de análisis.
2. Sistemas de visualización.
3. Comunicación segura.
4. Respaldo eléctrico.
5. Redes protegidas.
6. Protocolos de acceso.
7. Registro de operadores.

8. Monitoreo en tiempo real

Determinados sistemas críticos podrán generar información en tiempo real. Por ejemplo:

1. Detección de dispositivo.
2. Falla de bloqueador.
3. Manipulación de cámara.
4. Apertura no autorizada de puerta.
5. Falla eléctrica.
6. Alerta perimetral.

El Centro deberá clasificar las alertas según importancia.

9. Clasificación de alertas

Las alertas podrán organizarse por niveles.

Nivel Verde

Evento informativo. No requiere intervención inmediata.

Nivel Amarillo

Evento anormal que requiere verificación.

Nivel Naranja

Incidente que requiere actuación operacional.

Nivel Rojo

Evento de alta gravedad relacionado con seguridad inmediata, actividad criminal o falla crítica.

Los criterios deberán establecerse mediante protocolos nacionales.

RD Propone RD Propone

10. Prevención de saturación

El sistema deberá evitar generar cantidades excesivas de alertas sin valor operativo.

Una plataforma que produce continuamente falsas alarmas puede ocasionar que eventos importantes sean ignorados. Por ello deberán medirse:

- Tasa de falsas alertas.
- Alertas repetitivas.
- Tiempo de respuesta.
- Alertas cerradas sin incidencia.

Los parámetros deberán ajustarse periódicamente.

11. Correlación automática de eventos

El Centro deberá desarrollar capacidades para relacionar diferentes eventos. Por ejemplo:

18:42 *Dispositivo celular detectado.*

18:44 *Actividad eléctrica anormal.*

18:46 *Cámara registra movimiento.*

18:51 *Apertura de puerta de acceso.*

El sistema podrá marcar estos eventos como relacionados. La correlación no constituirá prueba automática de responsabilidad.

12. Línea temporal nacional

Cada incidente relevante deberá poder reconstruirse cronológicamente. La línea temporal podrá integrar:

- Registros de acceso.
- Cámaras.
- Alertas celulares.
- Alarmas eléctricas.
- Eventos del sistema.
- Decomisos.
- Reportes de funcionarios.

13. Identificación de reincidencias

RD Propone RD Propone

La plataforma deberá identificar cuando determinados elementos aparezcan repetidamente. Podrán incluirse:

1. IMEI.
2. SIM.
3. Número telefónico.
4. Método de ocultamiento.
5. Proveedor.
6. Vehículo.
7. Punto de ingreso.
8. Área interna.
9. Tipo de cargador.
10. Modificación eléctrica.

La reincidencia deberá generar análisis adicional.

14. Análisis entre centros penitenciarios

Una de las principales ventajas del sistema nacional será comparar establecimientos. Por ejemplo, podrá detectarse que:

- Un mismo dispositivo aparece asociado a más de un centro.
- Una modalidad de introducción utilizada inicialmente en una prisión aparece posteriormente en otra.
- Un proveedor presta servicios en varios establecimientos donde ocurren incidentes similares.
- Una nueva técnica de ocultamiento comienza a propagarse.

Esto permitirá respuestas preventivas nacionales.

15. Inteligencia anticipativa

La información acumulada deberá utilizarse para anticipar riesgos. El Centro podrá identificar tendencias como:

1. Aumento progresivo de dispositivos.
2. Cambio de horarios.
3. Migración hacia nuevas tecnologías.
4. Mayor utilización de baterías externas.
5. Nuevas rutas de ingreso.

RD Propone RD Propone

6. Uso de drones.
7. Modificaciones eléctricas recurrentes.

La función será anticipar, no únicamente reaccionar.

16. Mapas de riesgo

Cada establecimiento deberá contar con mapas internos de riesgo actualizados. Estos podrán identificar áreas según:

1. Decomisos.
2. Alertas.
3. Puntos ciegos.
4. Manipulaciones.
5. Actividad celular.
6. Actividad eléctrica.
7. Accesos.
8. Incidentes históricos.

Los mapas deberán servir para orientar inversiones y operaciones.

17. Mapa nacional de riesgo penitenciario

La clasificación deberá considerar múltiples factores. No deberá basarse únicamente en la cantidad de teléfonos encontrados, debido a que un mayor número de decomisos podría reflejar mejores controles.

18. Índice compuesto de riesgo tecnológico

Podrá desarrollarse un indicador nacional que combine:

1. Dispositivos detectados.
2. Dispositivos decomisados.
3. Intentos de introducción.
4. Actividad radioeléctrica no autorizada.
5. Manipulaciones eléctricas.
6. Fallos tecnológicos.
7. Incidentes vinculados a personal.
8. Reincidencia.

19. Análisis de tendencias

RD Propone RD Propone

El Centro deberá elaborar informes:

1. Semanalmente.
2. Mensualmente.
3. Trimestralmente.
4. Anualmente.

Los informes deberán mostrar tendencias y no simplemente cantidades acumuladas.

20. Alertas tempranas

Cuando determinados indicadores superen parámetros previamente establecidos, el sistema podrá generar alertas tempranas. Por ejemplo:

1. Aumento abrupto de teléfonos encontrados.
2. Fallas repetidas de bloqueadores.
3. Cámaras desactivadas frecuentemente.
4. Incremento de manipulaciones eléctricas.
5. Repetición de incidentes en un acceso.

Esto permitirá intervenir antes de que la vulnerabilidad se consolide.

21. Inteligencia sobre introducción

El Centro deberá estudiar cómo ingresan los dispositivos. Las modalidades deberán clasificarse. Por ejemplo:

1. Visitantes.
2. Personal.
3. Proveedores.
4. Vehículos.
5. Paquetes.
6. Drones.
7. Lanzamientos.
8. Construcción.
9. Ocultamiento en alimentos.
10. Otros.

La clasificación permitirá determinar qué controles producen mejores resultados.

22. Base nacional de decomisos

RD Propone RD Propone

Todo decomiso deberá incorporarse a una plataforma nacional. El registro deberá permitir conocer:

1. Centro.
2. Zona.
3. Fecha.
4. Hora.
5. Tipo de dispositivo.
6. Marca.
7. Modelo.
8. IMEI cuando sea posible.
9. SIM.
10. Accesorios.
11. Método de ocultamiento.
12. Persona relacionada cuando corresponda.
13. Ruta probable de ingreso.
14. Estado de investigación.

23. Identificador único de incidente

Cada incidente deberá recibir un número único. Ese número acompañará:

1. Reporte.
2. Fotografías.
3. Video.
4. Evidencia.
5. Investigación.
6. Cadena de custodia.
7. Medidas correctivas.

Esto evitará que la información quede fragmentada entre distintos sistemas.

24. Gestión de casos

Los incidentes relevantes deberán poder convertirse en expedientes digitales.

El sistema deberá mostrar, estado, funcionario responsable, investigación iniciada, acciones pendientes, documentos, evidencias, fecha límite y resultado. El expediente no deberá cerrarse simplemente porque el teléfono fue decomisado.

RD Propone RD Propone

25. Investigación de causa raíz

Cada incidente relevante deberá procurar determinar su causa. El análisis deberá responder:

1. ¿Cómo ingresó?
2. ¿Qué control falló?
3. ¿Dónde estuvo?
4. ¿Cómo obtuvo energía?
5. ¿Cómo consiguió señal?
6. ¿Quién pudo acceder al área?
7. ¿Qué medida impediría repetir el incidente?

Este análisis deberá producir recomendaciones.

26. Medidas correctivas

Los incidentes deberán generar acciones concretas. Por ejemplo:

1. Mover una cámara.
2. Cambiar protocolo.
3. Reparar bloqueador.
4. Eliminar punto eléctrico vulnerable.
5. Modificar ruta de mercancías.
6. Cambiar procedimiento de visitas.
7. Realizar auditoría.
8. Capacitar personal.

Cada acción deberá quedar asociada al incidente que la originó.

27. Seguimiento de medidas correctivas

El Centro deberá verificar si las recomendaciones fueron ejecutadas. El sistema podrá mostrar:

1. Pendiente.
2. En ejecución.
3. Completada.
4. Verificada.
5. No aceptada.

RD Propone RD Propone

Toda decisión de no ejecutar una recomendación importante deberá ser motivada.

28. Inteligencia sobre redes criminales

Cuando existan indicios de que dispositivos clandestinos están relacionados con delitos externos, la información deberá compartirse con las autoridades investigativas competentes conforme al marco legal.

La inteligencia penitenciaria puede aportar información sobre:

1. Contactos.
2. Patrones.
3. Reincidencias.
4. Relaciones entre internos.
5. Rutas de suministro.
6. Eventos tecnológicos.

Pero la investigación penal corresponderá a las autoridades legalmente competentes.

29. Límites de la inteligencia penitenciaria

El Centro no deberá convertirse en un sistema de vigilancia general sobre toda la población. Su actuación deberá limitarse a finalidades penitenciarias y de seguridad legalmente definidas.

Los datos de personas externas deberán tratarse conforme a las normas de privacidad, protección de datos y debido proceso.

30. Acceso segmentado a información

No todos los usuarios deberán visualizar la totalidad de los datos, los permisos deberán organizarse por función. Por ejemplo:

- Director de centro.
- Analista nacional.
- Técnico.
- Investigador autorizado.
- Auditor.
- Administrador tecnológico.

Cada perfil deberá disponer únicamente del acceso necesario.

RD Propone RD Propone

31. Registro de auditoría

Toda actividad relevante realizada dentro del sistema deberá quedar registrada. Deberá conocerse:

1. Usuario.
2. Hora.
3. Información consultada.
4. Cambio realizado.
5. Archivo descargado.
6. Registro eliminado.
7. Autorización concedida.

Esto permitirá detectar usos indebidos.

32. Inmutabilidad de registros críticos

Determinados registros deberán protegerse contra alteraciones posteriores. Tales como:

1. Decomisos.
2. Incidentes.
3. Alertas.
4. Cadena de custodia.
5. Modificaciones administrativas.

Podrán utilizarse mecanismos tecnológicos que permitan verificar si la información fue alterada.

33. Ciberseguridad

El Centro deberá considerarse infraestructura crítica, por lo que sus sistemas deberán protegerse frente a:

1. Intrusiones.
2. Malware.
3. Robo de credenciales.
4. Ataques externos.
5. Sabotaje interno.
6. Manipulación de registros.
7. Pérdida de información.

RD Propone RD Propone

Deberán aplicarse mecanismos de seguridad acordes con el nivel de sensibilidad.

34. Autenticación reforzada

Los usuarios con acceso a sistemas sensibles deberán utilizar mecanismos de autenticación reforzada.

Especial atención deberá prestarse a cuentas administrativas. Las credenciales no deberán compartirse.

35. Segmentación de redes

Los sistemas de seguridad deberán mantenerse separados, cuando técnicamente resulte posible, de redes administrativas ordinarias.

La segmentación reducirá el impacto potencial de una intrusión.

36. Copias de seguridad

La información crítica deberá contar con copias de seguridad, deberán almacenarse de forma segura y verificarse periódicamente. El Centro deberá disponer de procedimientos de recuperación ante desastre.

37. Continuidad operativa

Deberán existir planes para mantener funciones críticas ante la ocurrencia de apagones, fallas de internet, ataques informáticos, Incendios, desastres naturales o fallas de servidores. El sistema deberá disponer de redundancia razonable.

38. Protección física

El acceso físico a servidores, salas técnicas y áreas de monitoreo deberá estar restringido. Podrán utilizarse:

1. Credenciales.
2. Registro de entrada.
3. Cámaras.
4. Controles de visitantes.
5. Inventario de equipos.

39. Personal especializado

El Centro deberá contar con equipos multidisciplinarios. Podrán incluir:

RD Propone RD Propone

1. Analistas.
2. Ingenieros.
3. Especialistas en telecomunicaciones.
4. Especialistas en ciberseguridad.
5. Personal penitenciario.
6. Expertos en análisis de datos.
7. Personal jurídico.
8. Auditores.

La combinación permitirá interpretar adecuadamente los datos.

40. Capacitación continua

La tecnología y las modalidades criminales evolucionan, por ello, el personal deberá recibir capacitación periódica, incluyendo programas de:

- Análisis de datos.
- Telecomunicaciones.
- Seguridad penitenciaria.
- Ciberseguridad.
- Cadena de custodia.
- Protección de datos.
- Derechos fundamentales.
- Nuevas modalidades de contrabando.

41. Inteligencia artificial

Podrán utilizarse herramientas de inteligencia artificial para apoyar:

1. Clasificación de alertas.
2. Detección de anomalías.
3. Búsqueda de patrones.
4. Análisis de grandes volúmenes de información.
5. Correlación de eventos.
6. Priorización de incidentes.

42. Supervisión humana

Ninguna persona deberá ser sancionada o considerada responsable únicamente por una conclusión automatizada. Los modelos deberán generar indicadores y recomendaciones.

RD Propone RD Propone

Las decisiones deberán permanecer bajo responsabilidad humana.

43. Evaluación de algoritmos

Los sistemas automatizados deberán evaluarse periódicamente. La evaluación deberá analizar:

1. Precisión.
2. Falsos positivos.
3. Falsos negativos.
4. Sesgos.
5. Utilidad.
6. Rendimiento.
7. Riesgos.

Los modelos que no produzcan resultados confiables deberán corregirse o retirarse.

44. Interoperabilidad

Los sistemas adquiridos deberán poder intercambiar información mediante estándares técnicos apropiados.

La política deberá evitar depender permanentemente de un solo proveedor tecnológico. Los datos deberán permanecer bajo control del Estado.

45. Propiedad pública de los datos

Los contratos deberán establecer claramente que la información penitenciaria producida mediante sistemas financiados por el Estado pertenece al Estado dominicano.

Los proveedores no podrán apropiarse ni comercializar datos generados por el sistema.

46. Integración con INDOTEL

INDOTEL deberá participar técnicamente en los componentes relacionados con telecomunicaciones.

La institución ya ha desarrollado iniciativas de inhibición de señal penitenciaria en coordinación con el sistema de justicia, incluyendo acuerdos para la instalación de equipos en centros penitenciarios.

El Centro deberá recibir información técnica suficiente para conocer el estado de estos sistemas sin invadir competencias regulatorias.

RD Propone RD Propone

47. Coordinación con el Ministerio de Justicia

El Ministerio de Justicia deberá ejercer la coordinación estratégica correspondiente sobre la política penitenciaria nacional, de acuerdo con la reorganización institucional vigente.

El Centro deberá proporcionar información objetiva para apoyar decisiones presupuestarias, operativas y de política pública.

48. Coordinación con el Ministerio Público

Cuando la información produzca indicios razonables de hechos delictivos, deberá existir un protocolo de remisión. El Centro no sustituirá las funciones constitucionales de investigación penal, su función será preservar y suministrar la información correspondiente conforme a la ley.

49. Informes estratégicos

Además de monitorear operaciones diarias, el Centro deberá producir análisis estratégicos. Estos podrán abordar:

1. Evolución de comunicaciones ilícitas.
2. Nuevas tecnologías utilizadas.
3. Rutas de contrabando.
4. Impacto de bloqueadores.
5. Impacto de controles eléctricos.
6. Participación de personal.
7. Costos.
8. Resultados.
9. Necesidades de inversión.

50. Informe anual de seguridad tecnológica penitenciaria

El informe podrá incluir información agregada sobre:

1. Dispositivos decomisados.
2. Intentos de ingreso.
3. Tecnologías implementadas.
4. Resultados.
5. Fallos.
6. Inversiones.
7. Auditorías.

RD Propone RD Propone

8. Mejoras.

No deberá publicarse información cuya divulgación comprometa la seguridad operacional.

51. Transparencia diferenciada

La política deberá distinguir entre información que debe ser pública y aquella cuya divulgación aumentaría vulnerabilidades. Serán generalmente transparentes:

1. Presupuestos.
2. Contratos.
3. Resultados generales.
4. Indicadores.
5. Auditorías financieras.

Serán protegidos, cuando corresponda:

1. Configuraciones técnicas.
2. Puntos ciegos.
3. Frecuencias específicas.
4. Ubicación de determinados equipos.
5. Métodos de detección.
6. Protocolos de respuesta sensibles.

52. Auditoría independiente

El Centro deberá someterse periódicamente a auditorías. Estas deberán evaluar:

1. Funcionamiento.
2. Seguridad informática.
3. Protección de datos.
4. Calidad de información.
5. Controles de acceso.
6. Resultados.
7. Cumplimiento legal.

La unidad que opera el sistema no deberá ser la única que evalúe su desempeño.

53. Indicadores de desempeño

Se deberán medir:

RD Propone RD Propone

1. Número de alertas.
2. Porcentaje verificadas.
3. Tiempo de respuesta.
4. Incidentes correlacionados.
5. Patrones identificados.
6. Rutas de ingreso descubiertas.
7. Medidas correctivas ejecutadas.
8. Fallos detectados.
9. Falsas alarmas.
10. Investigaciones apoyadas.
11. Reincidencia.

54. Evaluación costo-beneficio

La tecnología deberá evaluarse por resultados. No deberá asumirse que una plataforma costosa es necesariamente efectiva. Cada sistema deberá demostrar utilidad mediante indicadores. Las tecnologías que generen costos elevados sin resultados suficientes deberán reconsiderarse.

55. Implementación progresiva

El Centro podrá desarrollarse por fases.

Primera fase	Integración de decomisos, accesos y estadísticas.
Segunda fase	Integración de cámaras, telecomunicaciones y alertas eléctricas.
Tercera fase	Correlación avanzada de eventos.
Cuarta fase	Analítica predictiva y automatización controlada.

La expansión deberá producirse después de evaluar cada etapa.

56. Centros piloto

Antes de desplegar todas las capacidades a escala nacional, deberán utilizarse establecimientos piloto. La selección podrá considerar:

1. Tamaño.
2. Infraestructura.
3. Nivel de incidencia.

RD Propone RD Propone

4. Disponibilidad tecnológica.
5. Diversidad regional.

Las lecciones aprendidas deberán aplicarse a la expansión.

57. Incorporación de nuevos centros

La República Dominicana se encuentra actualmente ampliando su infraestructura penitenciaria con nuevos Centros de Corrección y Rehabilitación; durante 2026 el Gobierno ha iniciado múltiples instalaciones nuevas como parte del proceso de modernización del sistema.

Estos nuevos centros representan una oportunidad para incorporar desde su construcción la infraestructura necesaria para integrarse al sistema nacional de monitoreo, en lugar de instalarla posteriormente.

58. Laboratorio tecnológico penitenciario

Podrá establecerse dentro del Centro una pequeña unidad de evaluación tecnológica. Su propósito será probar nuevas soluciones antes de realizar adquisiciones nacionales. Podrán evaluarse:

1. Detectores.
2. Cámaras.
3. Sistemas eléctricos.
4. Software.
5. Bloqueadores.
6. Sistemas de acceso administrado.
7. Sensores.
8. Herramientas de análisis.

Esto reducirá el riesgo de adquirir tecnologías poco efectivas.

59. Cooperación académica

El sistema podrá establecer acuerdos con universidades e instituciones técnicas. La cooperación podrá incluir:

1. Análisis de datos.
2. Ciberseguridad.
3. Ingeniería.

RD Propone RD Propone

4. Evaluación de tecnologías.
5. Formación.
6. Investigación.

Los datos sensibles deberán permanecer protegidos.

60. Resultado esperado

El Centro Nacional deberá convertirse en el punto donde las diferentes capas de seguridad penitenciaria se transformen en un sistema coherente. Un teléfono clandestino podrá generar sucesivamente:

Detección de señal / Alerta / Ubicación aproximada / Correlación con cámaras / Revisión de accesos / Inspección / Decomiso / Registro / Investigación de origen / Identificación de vulnerabilidad / Medida correctiva / Seguimiento.

El propósito será abandonar un modelo reactivo en el cual cada teléfono decomisado constituye un incidente aislado.

La República Dominicana deberá avanzar hacia un modelo en el cual cada incidente produzca información, cada información produzca aprendizaje y cada aprendizaje fortalezca permanentemente el sistema penitenciario.

CAPÍTULO X
AUDITORÍA, PRUEBAS, CERTIFICACIÓN Y EVALUACIÓN PERMANENTE DEL SISTEMA DE SEGURIDAD PENITENCIARIA

1. Objeto

El presente capítulo establece un sistema permanente de auditoría, pruebas, certificación y evaluación destinado a comprobar que los mecanismos de seguridad instalados en los establecimientos penitenciarios funcionan efectivamente.

La existencia física de cámaras, detectores, sistemas de control de telecomunicaciones, controles eléctricos, puertas, sensores u otros dispositivos no será considerada suficiente para acreditar el cumplimiento de las condiciones de seguridad. Deberá demostrarse periódicamente su funcionamiento.

2. Principio de seguridad verificable

Todo mecanismo crítico de seguridad deberá poder ser sometido a una prueba objetiva. La autoridad responsable deberá poder responder:

RD Propone RD Propone

1. ¿Está instalado?
2. ¿Está funcionando?
3. ¿Está siendo utilizado correctamente?
4. ¿Está siendo monitoreado?
5. ¿Qué ocurre cuando falla?
6. ¿Cuánto tiempo tarda en ser reparado?

Este principio deberá aplicarse a todos los centros del sistema.

3. Certificación periódica de seguridad

Cada establecimiento deberá obtener periódicamente una certificación de cumplimiento de sus sistemas críticos de seguridad. La certificación deberá comprobar, como mínimo:

a) Funcionamiento de sistemas de detección;

b) Funcionamiento de sistemas de control de telecomunicaciones;

c) Estado de cámaras;

d) Control de accesos;

e) Integridad de registros;

f) Sistemas eléctricos críticos;

g) Sistemas de respaldo;

h) Protocolos de respuesta;

i) Capacitación del personal;

j) Procedimientos de inspección.

4. Certificación no permanente

Ninguna certificación deberá considerarse indefinida. La seguridad tecnológica puede deteriorarse por:

1. Desgaste.
2. Daños.
3. Cambios tecnológicos.
4. Modificaciones estructurales.
5. Interferencias.

RD Propone RD Propone

6. Errores humanos.
7. Nuevas modalidades criminales.

Por ello, la certificación deberá renovarse periódicamente.

5. Pruebas funcionales

Los sistemas deberán someterse a pruebas funcionales programadas. Estas deberán determinar si cada componente realiza efectivamente la función para la cual fue adquirido. Por ejemplo:

- Una cámara deberá demostrar que registra correctamente.
- Un sensor deberá demostrar que detecta el evento para el cual fue instalado.
- Un sistema de control de telecomunicaciones deberá demostrar que mantiene las condiciones de funcionamiento establecidas.

6. Pruebas sorpresa

Además de las inspecciones programadas, deberán realizarse pruebas no anunciadas. Su finalidad será verificar que los sistemas no sean preparados artificialmente únicamente para recibir una inspección previamente conocida.

Las pruebas sorpresa deberán ser realizadas conforme a protocolos que eviten afectar innecesariamente la seguridad del establecimiento.

7. Equipo independiente de auditoría

Las auditorías críticas no deberán depender exclusivamente del personal que administra directamente los sistemas evaluados.

Deberá existir una capacidad de auditoría independiente dentro de la estructura estatal.

Cuando corresponda, podrán contratarse evaluadores externos especializados bajo condiciones que protejan la información sensible.

8. Prohibición de certificación basada únicamente en documentos

No podrá considerarse que un sistema funciona simplemente porque:

1. Existe una factura.
2. Existe un contrato.
3. Existe un informe del proveedor.
4. Existe una fotografía del equipo.

RD Propone RD Propone

5. Existe un acta de instalación.

La certificación deberá incorporar evidencia funcional.

9. Pruebas de disponibilidad

Deberá medirse cuánto tiempo permanece disponible cada sistema crítico, para lo que se establecerán indicadores de:

1. Disponibilidad.
2. Interrupciones.
3. Duración de fallas.
4. Frecuencia de fallas.
5. Tiempo de reparación.
6. Reincidencia de fallas.

10. Tiempo máximo de reparación

Los contratos de mantenimiento deberán establecer tiempos máximos razonables para atender fallas críticas. La prioridad dependerá de la función del equipo.

Una falla que comprometa una barrera esencial de seguridad deberá recibir tratamiento diferente a una falla de carácter administrativo.

11. Registro nacional de fallas

Todas las fallas relevantes deberán registrarse en el sistema nacional. El registro deberá incluir:

1. Equipo.
2. Centro.
3. Fecha.
4. Hora.
5. Tipo de falla.
6. Duración.
7. Proveedor responsable.
8. Acción correctiva.
9. Fecha de reparación.
10. Resultado de la prueba posterior.

12. Reincidencia de fallas

RD Propone RD Propone

Cuando un equipo presente fallas repetidas, deberá analizarse si resulta conveniente:

1. Repararlo.
2. Sustituirlo.
3. Rediseñar la instalación.
4. Cambiar proveedor.
5. Modificar el protocolo.

La reparación permanente de un sistema que continúa fallando no deberá considerarse automáticamente una solución satisfactoria.

13. Pruebas de cámaras

Las cámaras deberán evaluarse respecto de:

1. Calidad de imagen.
2. Cobertura.
3. Grabación.
4. Almacenamiento.
5. Fecha y hora.
6. Visibilidad nocturna.
7. Disponibilidad.
8. Integridad de archivos.

Las áreas críticas deberán revisarse para determinar la existencia de puntos ciegos.

14. Control de puntos ciegos

Los establecimientos deberán mantener un mapa actualizado de cobertura de videovigilancia. Los puntos ciegos deberán clasificarse según su importancia.

Cuando un punto ciego sea considerado crítico deberá establecerse una medida correctiva.

15. Integridad de grabaciones

Los sistemas deberán impedir, dentro de lo técnicamente razonable, la eliminación o modificación no autorizada de grabaciones.

Las acciones administrativas sobre archivos sensibles deberán quedar registradas.

16. Retención de imágenes

RD Propone RD Propone

Deberán establecerse períodos de conservación diferenciados según:

1. Tipo de cámara.
2. Zona.
3. Nivel de seguridad.
4. Incidente.
5. Investigación.
6. Requisitos legales.

Las grabaciones asociadas a incidentes deberán conservarse durante el tiempo necesario conforme a la normativa aplicable.

17. Pruebas de sistemas de telecomunicaciones

Los sistemas destinados a impedir o controlar comunicaciones no autorizadas deberán ser evaluados periódicamente. Determinando si:

1. Funcionan conforme a especificaciones.
2. Existen zonas con cobertura insuficiente.
3. Existen interferencias no previstas.
4. Existen equipos fuera de servicio.

Las condiciones han cambiado debido a nuevas construcciones o tecnologías.

18. Evaluación independiente del sistema de control de señal

Los resultados reportados por el proveedor no deberán constituir por sí solos la certificación final. La autoridad podrá contratar o designar evaluadores técnicamente independientes para verificar el comportamiento real del sistema.

19. Evolución tecnológica

Las pruebas deberán actualizarse conforme aparezcan nuevas tecnologías de comunicación.

El hecho de que un sistema haya funcionado correctamente durante un período determinado no garantiza que continúe siendo suficiente frente a tecnologías posteriores.

20. Control sobre dispositivos de prueba

Las pruebas de seguridad deberán utilizar procedimientos documentados y dispositivos autorizados. Los equipos empleados para realizar pruebas deberán estar inventariados.

RD Propone RD Propone

Su uso deberá quedar registrado. Esto evitará que los propios mecanismos de prueba se conviertan en una vulnerabilidad.

21. Pruebas de controles eléctricos

Los sistemas eléctricos asociados a seguridad deberán ser revisados periódicamente. Deberá comprobarse:

1. Integridad.
2. Continuidad.
3. Protección.
4. Respaldo.
5. Alarmas.
6. Circuitos críticos.
7. Capacidad de detectar manipulaciones.

Las pruebas deberán ser realizadas por personal técnicamente competente.

22. Seguridad eléctrica diferenciada

La infraestructura eléctrica destinada a alimentar equipos de seguridad deberá estar claramente identificada.

Los sistemas críticos deberán disponer de mecanismos que permitan determinar rápidamente si una interrupción proviene de:

Falla de suministro.

1. Falla interna.
2. Manipulación.
3. Mantenimiento.
4. Daño deliberado.

23. Sistemas de respaldo

Los equipos críticos deberán contar, cuando corresponda, con mecanismos de respaldo. Podrán incluir:

1. Generadores.
2. UPS.
3. Baterías.
4. Sistemas redundantes.

RD Propone RD Propone

5. Enlaces alternativos.

La capacidad deberá definirse según la criticidad del sistema.

24. Pruebas de pérdida de energía

Los establecimientos deberán realizar pruebas controladas para determinar qué sucede cuando se pierde el suministro eléctrico. Deberá verificarse que los sistemas críticos:

1. Continúen funcionando.
2. Generen alertas.
3. Registren el evento.
4. Cambien correctamente al sistema de respaldo.
5. Recuperen su funcionamiento normal posteriormente.

25. Control de mantenimiento

Todo mantenimiento deberá quedar registrado, identificando:

1. Equipo.
2. Técnico.
3. Empresa.
4. Fecha.
5. Hora.
6. Trabajo realizado.
7. Componentes sustituidos.
8. Prueba posterior.

26. Mantenimiento no anunciado

En sistemas especialmente sensibles, podrán realizarse verificaciones para determinar que los equipos declarados como mantenidos efectivamente funcionan.

27. Auditoría de proveedores

Los proveedores de tecnología crítica estarán sujetos a mecanismos de supervisión contractual. Deberá evaluarse:

- Cumplimiento.
- Calidad.
- Tiempo de respuesta.
- Reincidencia de fallas.

RD Propone RD Propone

- Costos.
- Capacidad técnica.
- Seguridad de la información.

28. Penalidades contractuales

Los contratos podrán establecer consecuencias por:

1. Incumplimiento.
2. Retrasos injustificados.
3. Reportes incorrectos.
4. Fallas recurrentes no corregidas.
5. Manipulación de información.
6. Incumplimiento de estándares de seguridad.

Estas consecuencias deberán establecerse previamente en los contratos.

29. Prohibición de manipulación de informes

Será especialmente grave alterar deliberadamente informes destinados a demostrar el funcionamiento de un sistema de seguridad.

Cuando corresponda, la conducta deberá ser remitida a las autoridades competentes.

30. Auditoría cruzada

Los resultados de una auditoría podrán compararse con:

1. Registros electrónicos.
2. Grabaciones.
3. Reportes de incidentes.
4. Decomisos.
5. Órdenes de mantenimiento.
6. Registros de acceso.

Esta comparación permitirá detectar inconsistencias.

31. Sistema de doble evidencia

Para sistemas particularmente críticos se procurará que la condición reportada pueda verificarse mediante más de una fuente. Por ejemplo:

Reporte técnico + Registro electrónico o Certificación del proveedor + Prueba independiente.

RD Propone RD Propone

32. Pruebas de penetración institucional

Podrán realizarse ejercicios controlados destinados a determinar si una persona autorizada podría vulnerar los controles utilizando únicamente los medios que razonablemente tendría disponibles. Estos ejercicios deberán ser:

1. Autorizados.
2. Documentados.
3. Controlados.
4. Limitados.

Posteriormente deberán producir recomendaciones.

33. Equipos de prueba autorizados

Los ejercicios de seguridad deberán realizarse únicamente por equipos previamente autorizados. La identidad de sus integrantes podrá mantenerse reservada cuando la naturaleza del ejercicio lo requiera.

34. Objetivo de las pruebas

Las pruebas no deberán orientarse a castigar al personal.

Su finalidad será descubrir vulnerabilidades antes de que sean aprovechadas por organizaciones criminales.

35. Pruebas de cadena de ingreso

El sistema podrá realizar ejercicios destinados a evaluar controles de:

1. Visitantes.
2. Proveedores.
3. Mercancías.
4. Vehículos.
5. Personal.
6. Correspondencia.
7. Objetos autorizados.

La metodología deberá ser controlada para no introducir riesgos reales.

36. Evaluación de controles humanos

RD Propone RD Propone

La tecnología no deberá ser el único objeto de auditoría, también deberá evaluarse si el personal:

1. Cumple procedimientos.
2. Verifica credenciales.
3. Registra incidencias.
4. Realiza inspecciones.
5. Reporta anomalías.
6. Protege evidencia.
7. Cumple horarios.
8. Respeta protocolos.

37. Rotación de auditores

Para reducir familiaridad excesiva con los centros auditados, se podrán establecer mecanismos de rotación de los equipos de auditoría.

38. Informe de auditoría

Toda auditoría deberá producir un informe que incluya:

1. Hallazgos.
2. Nivel de gravedad.
3. Evidencias.
4. Recomendaciones.
5. Responsables.
6. Plazos.
7. Estado de cumplimiento.

Clasificación de hallazgos

Los hallazgos podrán clasificarse como:

Crítico Compromete directamente una función esencial de seguridad.

Alto Representa una vulnerabilidad significativa.

Medio Requiere corrección programada.

Bajo Representa una deficiencia administrativa o técnica de menor impacto.

40. Plan obligatorio de corrección

RD Propone RD Propone

Los hallazgos críticos y altos deberán generar un plan de corrección. El plan deberá establecer:

1. Acción.
2. Responsable.
3. Presupuesto cuando corresponda.
4. Fecha límite.
5. Mecanismo de verificación.

41. Seguimiento

Una auditoría no deberá considerarse cerrada simplemente porque se emitió el informe. Deberá verificarse posteriormente si las deficiencias fueron corregidas.

42. Reincidencia institucional

Cuando un centro presente repetidamente la misma vulnerabilidad, deberá realizarse una evaluación especial. La reincidencia podrá indicar:

1. Falta de recursos.
2. Mala administración.
3. Deficiencia técnica.
4. Problemas contractuales.
5. Falta de supervisión.
6. Corrupción.
7. una combinación de factores.

43. Responsabilidad administrativa

Cuando se determine que una deficiencia grave se mantuvo deliberadamente pese a advertencias y recursos disponibles, deberán evaluarse las responsabilidades administrativas correspondientes.

No deberá presumirse automáticamente responsabilidad individual.

44. Excepción documentada

Cuando una vulnerabilidad no pueda corregirse inmediatamente, deberá documentarse:

1. Motivo.
2. Riesgo.
3. Medidas temporales.

RD Propone RD Propone

4. Responsable.
5. Fecha prevista de solución.

La existencia de una excepción no deberá permitir que una vulnerabilidad quede indefinidamente sin resolver.

45. Semáforo nacional de cumplimiento

El sistema nacional podrá utilizar una clasificación operativa:

Verde: Cumplimiento satisfactorio.

Amarillo: Deficiencias que requieren atención.

Naranja: Vulnerabilidades importantes.

Rojo: Situación crítica que requiere intervención inmediata.

La clasificación deberá basarse en criterios objetivos y documentados.

46. Certificación especial para centros críticos

Los centros que presenten riesgos particularmente elevados podrán quedar sujetos a una frecuencia mayor de auditorías.

47. Indicadores públicos

La autoridad podrá publicar anualmente indicadores agregados sobre:

- Centros certificados.
- Auditorías realizadas.
- Fallas detectadas.
- Fallas corregidas.
- Tiempo promedio de reparación.
- Incidentes tecnológicos.
- Resultados de inspecciones.

La publicación deberá excluir información que comprometa la seguridad.

48. Informe al Ministerio de Justicia

El órgano responsable de la seguridad penitenciaria deberá presentar periódicamente al Ministerio de Justicia un informe consolidado sobre el estado de los sistemas.

Este informe deberá servir para determinar:

RD Propone RD Propone

1. Necesidades presupuestarias.
2. Prioridades.
3. Reparaciones.
4. Sustituciones.
5. Reformas.
6. Capacitación.

49. Vinculación con el presupuesto

La planificación presupuestaria deberá considerar los resultados de las auditorías.

Los equipos que presenten fallas recurrentes deberán ser priorizados para reparación o sustitución cuando corresponda.

50. Compras basadas en desempeño

Las futuras adquisiciones de tecnología de seguridad deberán considerar no solamente el precio de compra. También deberán evaluarse:

1. Costo de mantenimiento.
2. Disponibilidad.
3. Vida útil.
4. Capacidad de actualización.
5. Resultados de pruebas.
6. Garantías.
7. Soporte técnico.
8. Interoperabilidad.

51. Prueba previa a aceptación

Los sistemas nuevos no deberán considerarse definitivamente aceptados hasta superar las pruebas técnicas establecidas en el contrato.

La aceptación deberá basarse en desempeño comprobado.

52. Garantía y mantenimiento

Los contratos deberán establecer claramente:

1. Garantía.
2. Mantenimiento.
3. Repuestos.

RD Propone RD Propone

4. Tiempo de respuesta.
5. Actualizaciones.
6. Capacitación.
7. Soporte.
8. Condiciones de sustitución.

53. Independencia de la evaluación

Cuando un proveedor instale un sistema y posteriormente certifique por sí solo su funcionamiento, la administración deberá establecer mecanismos adicionales de verificación cuando la criticidad lo justifique.

54. Evaluación anual integral

Cada centro deberá someterse anualmente a una evaluación integral que combine:

1. Tecnología.
2. Infraestructura.
3. Personal.
4. Procedimientos.
5. Comunicaciones.
6. Auditoría.
7. Ciberseguridad.
8. Integridad institucional.

55. Revisión después de cada incidente grave

Todo incidente grave deberá producir una revisión extraordinaria. La pregunta principal no será únicamente:

¿Quién cometió el hecho?

También deberá preguntarse:

¿Qué permitió que ocurriera?

56. Principio de aprendizaje institucional

Los errores deberán convertirse en conocimiento institucional.

Cuando un incidente revele una vulnerabilidad que pueda existir en otros centros, la información deberá ser utilizada para prevenir su repetición a escala nacional.

RD Propone RD Propone

57. Banco nacional de vulnerabilidades

Podrá crearse un registro técnico nacional de vulnerabilidades identificadas. El registro deberá contener:

1. Tipo de vulnerabilidad.
2. Centro.
3. Fecha de detección.
4. Medida correctiva.
5. Resultado.
6. Aplicabilidad a otros centros.

58. Prohibición de ocultamiento

Ningún centro deberá ser incentivado a ocultar fallas para mantener artificialmente buenos indicadores. Los sistemas de evaluación deberán reconocer la identificación y corrección de vulnerabilidades.

59. Cultura de mejora continua

El modelo deberá evolucionar desde:

Instalar / Utilizar / Olvidar

Hacia

Instalar / Probar / Medir / Corregir / Volver a probar / Certificar / Monitorear / Mejorar.

60. Resultado esperado

El resultado final será establecer un principio sencillo:

Ningún sistema de seguridad penitenciaria deberá considerarse seguro porque fue instalado; deberá considerarse seguro porque ha demostrado, mediante pruebas independientes y periódicas, que funciona.

La política deberá convertir la seguridad penitenciaria en un proceso permanente de:

Prevención / Detección / Prueba / Auditoría / Corrección / Certificación / Seguimiento / Mejora continua.

De esta manera, las inversiones realizadas por el Estado no terminarán simplemente en equipos instalados, sino en capacidades de seguridad verificables y sostenibles.

RD Propone RD Propone

CAPÍTULO XI

RÉGIMEN DE INFRACCIONES, RESPONSABILIDADES Y REFORMAS LEGALES

1. Objeto

La presente propuesta establece un régimen integral de prevención, detección, investigación y sanción de las conductas relacionadas con el ingreso, posesión, suministro, utilización, ocultamiento, facilitación o manipulación de dispositivos electrónicos y sistemas de comunicación no autorizados dentro de los establecimientos penitenciarios y correccionales.

El objetivo no será únicamente castigar la posesión de un teléfono celular, sino desarticular la cadena que permite que un dispositivo no autorizado llegue al interior de un centro penitenciario y sea utilizado para actividades ilícitas.

El régimen deberá aplicarse respetando la Constitución, los derechos fundamentales, el debido proceso, la dignidad de las personas privadas de libertad y las garantías correspondientes a servidores públicos, visitantes, contratistas y demás personas sometidas a investigación.

2. Principio de responsabilidad diferenciada

La propuesta establecerá una clara diferenciación entre:

1. La persona privada de libertad que posea un dispositivo no autorizado.
2. La persona privada de libertad que utilice dicho dispositivo para actividades ilícitas.
3. La persona que introduzca físicamente el dispositivo al establecimiento.
4. La persona que financie, solicite, facilite o coordine su introducción.
5. El servidor público que permita deliberadamente su entrada o utilización.
6. El servidor público que omita controles obligatorios de manera deliberada.
7. El visitante, contratista o proveedor que participe en la introducción.
8. La persona externa que suministre dispositivos, tarjetas SIM, accesorios o mecanismos destinados a facilitar comunicaciones clandestinas.
9. La persona que manipule, inutilice o evada deliberadamente los sistemas de seguridad instalados para impedir estas conductas.
10. La persona que utilice una comunicación clandestina para ordenar, coordinar, financiar o facilitar la comisión de otros delitos.

RDPropone RDPropone

Cada conducta deberá recibir una consecuencia proporcional a su participación y al daño o riesgo generado.

3. Clasificación de las conductas

La normativa complementaria deberá establecer una clasificación clara de las conductas relacionadas con comunicaciones no autorizadas.

A. Posesión no autorizada

La tenencia de teléfonos celulares u otros dispositivos de comunicación no autorizados constituirá una infracción disciplinaria conforme al régimen penitenciario vigente, sin perjuicio de otras responsabilidades que pudieran derivarse de la conducta.

B. Utilización de dispositivo no autorizado

El uso deliberado de un dispositivo no autorizado constituirá una infracción diferenciada de la simple posesión, especialmente cuando existan evidencias de comunicaciones con personas externas.

C. Introducción

La introducción física de un dispositivo no autorizado a un establecimiento penitenciario deberá ser considerada una conducta de especial gravedad.

La normativa deberá distinguir entre:

- Introducción accidental
- Introducción por negligencia
- Introducción deliberada
- Introducción mediante pago o contraprestación
- Introducción coordinada con una persona privada de libertad
- Introducción destinada a facilitar actividades delictivas

D. Facilitación

Será considerada conducta especialmente grave cualquier acción destinada a facilitar que otra persona introduzca, conserve, utilice o recupere un dispositivo no autorizado. Se incluirán, entre otras conductas:

- Proporcionar dinero para adquirir el dispositivo
- Entregar el dispositivo
- Ocultarlo

RD Propone RD Propone

- Transportarlo
- Proporcionar una tarjeta SIM
- Proporcionar accesorios destinados a su funcionamiento;
- Proporcionar información para evadir controle
- Alterar registros
- Abrir accesos no autorizados
- Desactivar cámaras o sistemas de detección
- Advertir sobre operativos de inspección

E. Manipulación de los sistemas de seguridad

Deberá recibir tratamiento agravado cualquier conducta destinada a inutilizar, alterar, bloquear, engañar o evadir los sistemas tecnológicos destinados a proteger el establecimiento. Esto incluye los sistemas de:

- Videovigilancia
- Control de acceso
- Detección de dispositivos
- Telecomunicaciones
- Alarmas
- Registro electrónico
- Control eléctrico
- Almacenamiento de evidencias

4. Comunicaciones clandestinas vinculadas a delitos

Cuando una investigación determine que una comunicación realizada desde un dispositivo no autorizado estuvo destinada a coordinar, ordenar, financiar, amenazar, facilitar o encubrir otro hecho delictivo, la conducta deberá investigarse de manera independiente.

La posesión del dispositivo y el eventual delito cometido mediante su utilización deberán analizarse separadamente.

Esto permitirá evitar que el sistema penitenciario trate como una simple falta disciplinaria una conducta que pudiera constituir, además, una infracción penal.

5. Agravantes específicas

La legislación que se proponga deberá evaluar circunstancias agravantes cuando concurran, entre otras:

RD Propone RD Propone

1. Participación de un servidor público.
2. Participación de un funcionario con funciones de seguridad o custodia.
3. Recepción de dinero o beneficios.
4. Participación coordinada de varias personas.
5. Reincidencia.
6. Manipulación de cámaras o sistemas de seguridad.
7. Utilización de información privilegiada sobre los mecanismos de seguridad.
8. Participación de un contratista o proveedor.
9. Utilización del dispositivo para amenazar o intimidar a víctimas o testigos.
10. Utilización del dispositivo para coordinar otro delito.
11. Utilización del dispositivo para facilitar actividades de una estructura criminal.
12. Introducción de múltiples dispositivos.
13. Participación de personas externas organizadas para abastecer de dispositivos al establecimiento.

Las agravantes deberán aplicarse únicamente cuando sean establecidas por norma y acreditadas conforme al debido proceso.

6. Responsabilidad del personal penitenciario

El personal penitenciario tendrá una responsabilidad especial debido a las funciones de custodia, seguridad y control que desempeña.

Cuando un servidor público participe deliberadamente en la introducción o utilización de dispositivos no autorizados, además de las consecuencias penales que correspondan, deberá enfrentar el régimen disciplinario aplicable.

La investigación deberá determinar individualmente:

- Quién permitió el acceso;
- Quién tenía responsabilidad de inspección;
- Quién omitió el procedimiento;
- Quién alteró o dejó de registrar una incidencia;
- Quién recibió beneficios;
- Quién tenía conocimiento previo;
- Quién informó sobre los controles;
- Quién intervino posteriormente para ocultar evidencias.

No deberá establecerse responsabilidad automática por la simple ocurrencia de una infracción.

RD Propone RD Propone

La responsabilidad deberá surgir de hechos concretos, evidencia verificable y procedimiento legalmente establecido.

7. Responsabilidad por omisión deliberada

La normativa deberá diferenciar entre:
a) Error operativo o negligencia no deliberada, sujeto a los mecanismos administrativos correspondientes.
b) Omisión deliberada, cuando una persona, teniendo la obligación concreta de realizar un control, decide conscientemente no hacerlo con el propósito de permitir una infracción.
c) Complicidad, cuando exista coordinación o cooperación consciente para facilitar la conducta.
Esta diferenciación resulta fundamental para evitar tanto la impunidad como la imposición injustificada de responsabilidades.

8. Visitantes, contratistas y proveedores

El sistema deberá establecer un régimen específico para las personas que ingresen temporalmente a los establecimientos.

En función de la gravedad de la conducta acreditada podrán establecerse medidas tales como:

- Suspensión temporal de autorización de ingreso
- Cancelación de autorización
- Exclusión de determinados procesos de contratación, cuando legalmente proceda
- Remisión al Ministerio Público cuando existan indicios de infracción penal
- Responsabilidad contractual
- Reparación de daños cuando corresponda

La aplicación de estas medidas deberá garantizar el derecho de defensa y los recursos previstos por la legislación.

9. Cadena de custodia de dispositivos incautados

Todo dispositivo incautado deberá incorporarse a un procedimiento estandarizado de evidencia. El protocolo deberá establecer:

1. Identificación del dispositivo.
2. Registro fotográfico.

RD Propone RD Propone

3. Fecha, hora y lugar del hallazgo.
4. Persona que realizó la incautación.
5. Personas presentes.
6. Condiciones en que fue encontrado.
7. Embalaje y protección.
8. Registro de transferencia.
9. Almacenamiento seguro.
10. Análisis técnico autorizado.
11. Elaboración del informe.
12. Conservación o disposición final conforme a la ley.

Deberá evitarse la manipulación innecesaria del dispositivo. Cuando sea necesario analizar información almacenada en él, el procedimiento deberá respetar las reglas legales aplicables a la obtención y utilización de evidencia electrónica y a la protección de comunicaciones y datos personales.

10. Investigación tecnológica

La existencia de un dispositivo dentro de un centro penitenciario deberá considerarse potencialmente relevante para determinar:

- Su procedencia
- Quién lo introdujo
- Quién lo entregó
- Quién lo utilizó
- Cuándo comenzó a utilizarse
- Con qué números o identificadores estuvo asociado
- Si existieron otros dispositivos relacionados
- Si hubo comunicaciones con personas externas
- Si existe relación con investigaciones criminales abiertas

El análisis deberá realizarse por personal especializado y dentro de las facultades legales correspondientes.

11. Protección de la información y control judicial

El sistema de monitoreo penitenciario no deberá convertirse en un mecanismo de vigilancia indiscriminada. La propuesta deberá establecer una diferencia clara entre:

- Datos técnicos necesarios para la seguridad del establecimiento

RD Propone RD Propone

- Información operativa
- Metadatos
- Contenido de comunicaciones
- Información protegida por privilegio profesional o garantía legal

Cuando una actuación requiera autorización judicial, deberá obtenerse previamente conforme al procedimiento establecido por la legislación aplicable.

El objetivo será fortalecer la seguridad penitenciaria sin crear un sistema de vigilancia carente de límites jurídicos.

12. Registro nacional de incidentes

Se establecerá un registro nacional de incidentes relacionados con dispositivos y comunicaciones no autorizadas. Este registro deberá permitir identificar:

- Centro penitenciario;
- Fecha;
- Tipo de dispositivo;
- Lugar del hallazgo;
- Modalidad de ingreso;
- Persona vinculada al hallazgo;
- Resultado de la investigación;
- Existencia de participación interna;
- Existencia de participación externa;
- Reincidencia;
- Medidas adoptadas.

El registro deberá contar con controles de acceso, trazabilidad y protección de información.

13. Responsabilidad de los proveedores tecnológicos

Los contratos destinados a implementar sistemas de seguridad penitenciaria deberán incluir obligaciones específicas de:

- Disponibilidad
- Mantenimiento
- Actualización
- Protección de datos
- Ciberseguridad

RD Propone RD Propone

- Auditoría
- Trazabilidad
- Respuesta ante incidentes
- Conservación de registros
- Continuidad operacional

La contratación deberá evitar sistemas que dependan exclusivamente del proveedor sin mecanismos institucionales de supervisión. Los equipos críticos deberán someterse a pruebas de aceptación antes de ser recibidos formalmente por el Estado.

14. Régimen de sanciones institucionales

Cuando una investigación determine que una institución, unidad o responsable incumplió de forma sistemática controles obligatorios, deberán activarse mecanismos de:

- Auditoría;
- Investigación administrativa;
- Corrección inmediata;
- Capacitación;
- Sustitución de procedimientos;
- Responsabilidad individual cuando corresponda;
- Evaluación del contrato cuando intervenga un proveedor.

La existencia reiterada de dispositivos en un mismo establecimiento deberá generar automáticamente una revisión de vulnerabilidades.

15. Reformas legales necesarias

La implementación integral del presente programa deberá acompañarse de una revisión de:

1. La Ley núm. 113-21 sobre el Sistema Penitenciario y Correccional.
2. El Código Penal vigente.
3. La legislación procesal penal vigente.
4. El régimen disciplinario aplicable al personal público.
5. La normativa sobre telecomunicaciones.
6. La normativa sobre protección de datos personales.
7. Las normas de contratación pública.
8. Los reglamentos internos del sistema penitenciario.

RD Propone RD Propone

La finalidad de esta revisión será eliminar contradicciones, actualizar conceptos tecnológicos y establecer con precisión las responsabilidades que actualmente puedan encontrarse dispersas en distintas normas.

16. Prohibición de vacíos normativos

La reforma deberá evitar que una conducta quede sin respuesta jurídica debido a que el dispositivo utilizado sea diferente de un teléfono celular convencional. Por ello, deberán emplearse conceptos tecnológicamente neutrales que permitan abarcar, según corresponda:

- Teléfonos inteligentes
- Teléfonos convencionales
- Tabletas
- Dispositivos de mensajería
- Equipos de comunicación
- Dispositivos de acceso inalámbrico
- Sistemas equivalentes que permitan comunicación no autorizada.

La regulación deberá actualizarse periódicamente para evitar que la innovación tecnológica vuelva obsoleta la norma.

17. Régimen especial para la reincidencia

La reincidencia deberá ser incorporada como elemento de evaluación dentro del régimen disciplinario y, cuando corresponda conforme a la legislación penal, dentro de la determinación de responsabilidad. Deberán generarse alertas internas cuando una persona:

- Sea sorprendida repetidamente con dispositivos;
- Participe repetidamente en intentos de introducción;
- Sea vinculada a diferentes incidentes;
- Utilice diferentes dispositivos para evadir controles;
- Participe en redes internas de suministro.

La reincidencia no deberá presumirse: deberá estar documentada y legalmente acreditada.

18. Incentivos para la denuncia interna

RD Propone RD Propone

El sistema deberá establecer canales seguros y confidenciales para que internos, agentes, empleados administrativos, contratistas, visitantes autorizados, puedan informar sobre intentos de introducir dispositivos, corrupción o manipulación de los controles.

Cuando legalmente corresponda, deberán establecerse mecanismos de protección frente a represalias. La información recibida deberá ser sometida a evaluación profesional antes de adoptar medidas.

19. Principio de proporcionalidad

Las medidas disciplinarias y penales deberán guardar relación con:

- La gravedad de la conducta
- El nivel de participación
- El riesgo generado
- El daño producido
- La existencia de organización
- La reincidencia
- La utilización de la comunicación para otros delitos.

No deberá equipararse automáticamente la posesión de un dispositivo con la organización de una estructura criminal.

El sistema deberá perseguir con mayor intensidad las conductas que conviertan la infraestructura penitenciaria en una plataforma para la comisión de delitos desde el interior.

20. Evaluación periódica del régimen

Cada dos años deberá realizarse una evaluación integral del régimen de infracciones y sanciones para determinar:

- Cantidad de dispositivos incautados;
- Cantidad de intentos de introducción;
- Modalidades utilizadas;
- Participación del personal;
- Participación externa;
- Investigaciones iniciadas;
- Investigaciones concluidas;
- Sanciones impuestas;
- Procesos penales derivados;

RD Propone RD Propone

- Reincidencia;
- Eficacia de las medidas tecnológicas.

Los resultados deberán utilizarse para actualizar los protocolos, reglamentos y, cuando sea necesario, proponer nuevas modificaciones legislativas.

21. Principio rector de la reforma

La reforma no deberá descansar exclusivamente en el aumento de las penas. Su principio rector deberá ser:

Hacer difícil introducir el dispositivo, difícil conservarlo, difícil utilizarlo, difícil ocultarlo y fácil detectarlo; y cuando exista una conducta ilícita, hacer posible determinar quién la facilitó y responder ante la ley.

De esta manera, la política penitenciaria pasará de un modelo predominantemente reactivo a un modelo preventivo, tecnológico, trazable y basado en responsabilidades.

22. Disposición final propuesta

El Poder Ejecutivo, a través de las instituciones competentes, deberá elaborar los proyectos de modificación legislativa y reglamentaria necesarios para armonizar el presente programa con el ordenamiento jurídico nacional.

La implementación deberá realizarse de manera gradual, priorizando los establecimientos identificados como de mayor riesgo y estableciendo indicadores objetivos para medir sus resultados.

Ninguna medida tecnológica, disciplinaria o de vigilancia podrá aplicarse al margen de la Constitución, la ley y las garantías del debido proceso.

CAPÍTULO XII
MODELO TECNOLÓGICO INTEGRAL DE SEGURIDAD PENITENCIARIA

1. Finalidad

El Sistema Nacional de Seguridad Tecnológica Penitenciaria tendrá como finalidad impedir, detectar y documentar el ingreso y utilización de dispositivos de comunicación no autorizados dentro de los establecimientos penitenciarios, así como fortalecer la seguridad general de las instalaciones.

El sistema deberá diseñarse bajo un principio fundamental:

RD Propone RD Propone

Ninguna tecnología deberá constituir por sí sola el mecanismo de seguridad de un establecimiento penitenciario.

La seguridad deberá surgir de la combinación de infraestructura física, procedimientos humanos, tecnología, inteligencia, auditoría y capacidad de respuesta.

2. Arquitectura de seguridad por capas

Cada establecimiento deberá contar con varias capas independientes de protección:

Capa 1 Prevención física

- Controles de acceso;
- Inspección de personas;
- Inspección de objetos;
- Controles de vehículos;
- Areas de recepción;
- Separación de zonas;
- Perímetros de seguridad.

Capa 2 Detección tecnológica

- Detectores especializados;
- Sistemas de análisis del espectro;
- Sensores;
- Videovigilancia;
- Controles de acceso electrónicos;
- Sistemas de alarma.

Capa 3 Control de comunicaciones

- Comunicaciones institucionales autorizadas;
- Mecanismos técnicos para identificar comunicaciones no autorizadas;
- Coordinación con las autoridades competentes en telecomunicaciones;
- Monitoreo técnico dentro del marco legal.

Capa 4 Inteligencia y análisis

- Correlación de eventos;
- Análisis de patrones;
- Identificación de zonas recurrentes;
- Identificación de horarios críticos;

RD Propone RD Propone

- Análisis de incidentes;
- Investigación de redes de suministro.

Capa 5 Respuesta

- Alertas automáticas
- Intervención del personal
- Aislamiento de la zona
- Preservación de evidencia
- Investigación
- Comunicación a las autoridades correspondientes

3. Sistema Nacional de Videovigilancia Penitenciaria

Todos los establecimientos deberán evolucionar hacia una arquitectura de videovigilancia integrada. Las cámaras deberán cubrir, de acuerdo con la evaluación de riesgo:

- Entradas
- Salidas
- Perímetro
- Areas de recepción
- Puntos de inspección
- Areas de visita
- Corredores
- Zonas comunes
- Patios
- Talleres
- Almacenes
- Areas de servicio
- Zonas de transferencia
- Areas donde se almacenen bienes sensibles

No deberá existir una dependencia absoluta de la grabación. El sistema deberá permitir generar alertas ante determinados eventos previamente definidos.

4. Integridad de las cámaras

Toda cámara crítica deberá contar con mecanismos que permitan identificar:

- Pérdida de señal

RD Propone RD Propone

- Desconexión
- Manipulación
- Movimiento no autorizado
- Alteración de configuración
- Pérdida de almacenamiento
- Modificación de fecha y hora

Una cámara fuera de servicio deberá generar una alerta automática. La ausencia de imagen de una zona crítica no deberá considerarse simplemente una falla técnica ordinaria. Deberá quedar registrada como incidente de seguridad hasta determinar su causa.

5. Almacenamiento y conservación de imágenes

Las imágenes deberán almacenarse en sistemas protegidos contra alteraciones y con registros de auditoría. El sistema deberá registrar:

- Quién accedió;
- Cuándo accedió;
- Qué información consultó;
- Qué operación realizó;
- Si descargó información;
- Si exportó imágenes;
- Si realizó alguna modificación autorizada.

El período de conservación deberá determinarse según la criticidad del área, las necesidades operativas y las obligaciones legales aplicables. Las imágenes relacionadas con incidentes deberán preservarse conforme a los protocolos de evidencia.

6. Detección de dispositivos de comunicación

Los establecimientos deberán disponer de tecnología especializada para detectar la presencia o actividad de dispositivos de comunicación no autorizados.

La arquitectura podrá combinar diferentes tecnologías de detección, según las características del establecimiento. El objetivo no será únicamente responder a la pregunta **"¿Hay un teléfono?"** sino poder determinar:

- ¿En qué zona se encuentra?
- ¿Cuándo apareció?
- ¿Se ha detectado anteriormente?

RD Propone RD Propone

- ¿Es un evento aislado o recurrente?
- ¿Coincide con otros eventos?
- ¿Existen patrones de actividad?
- ¿Se ha producido una alerta similar anteriormente?

7. Sistema de localización por zonas

Cuando un sistema detecte una actividad sospechosa, deberá ser capaz, cuando la tecnología lo permita y dentro del marco legal, de aproximar la zona donde ocurre el evento. El objetivo será reducir considerablemente el tiempo entre:

Detección / Ubicación / Intervención / Incautación / Investigación

8. Coordinación con INDOTEL

Toda infraestructura tecnológica relacionada con radiofrecuencia, espectro radioeléctrico o telecomunicaciones deberá desarrollarse coordinadamente con el Instituto Dominicano de las Telecomunicaciones.

Antes de instalar sistemas que puedan afectar comunicaciones externas deberá realizarse una evaluación técnica y jurídica.

El Estado deberá evitar que una solución destinada a proteger un centro penitenciario genere interferencias perjudiciales sobre:

- Hospitales
- Viviendas
- Empresas
- Vehículos
- Servicios de emergencia
- Redes públicas
- Establecimientos ubicados alrededor del centro

9. Control técnico de las comunicaciones

El sistema podrá incorporar soluciones tecnológicas destinadas a identificar o impedir comunicaciones no autorizadas dentro del perímetro penitenciario, siempre que su utilización sea compatible con la legislación dominicana y las autorizaciones correspondientes.

La política tecnológica deberá priorizar soluciones que permitan:

1. Identificar

RD Propone RD Propone

2. Localizar
3. Clasificar
4. Alertar
5. Responder

Cuando sea técnicamente posible, deberán preferirse soluciones selectivas y controladas sobre mecanismos indiscriminados que puedan afectar a terceros.

10. No utilizar la infraestructura eléctrica como mecanismo de destrucción

La infraestructura eléctrica de los establecimientos deberá ser considerada un componente de seguridad, pero no deberá utilizarse para intentar destruir, dañar o inutilizar teléfonos celulares mediante descargas, sobretensiones u otros mecanismos similares. La red eléctrica deberá cumplir una función distinta:

- Garantizar seguridad
- Asegurar continuidad operacional
- Proteger equipos
- Detectar anomalías
- Alimentar sistemas críticos
- Permitir auditoría del consumo cuando resulte útil

Los sistemas de protección eléctrica deberán estar completamente separados de cualquier mecanismo destinado al control de comunicaciones. La seguridad tecnológica deberá buscar *detectar e impedir*, no provocar daños físicos a dispositivos mediante la infraestructura eléctrica.

11. Monitoreo inteligente de infraestructura

Los establecimientos podrán incorporar sensores destinados a detectar anomalías en:

- Consumo eléctrico
- Cpertura de puertas
- Funcionamiento de cámaras
- Sistemas de acceso
- Equipos de comunicación
- Temperatura de salas técnicas
- Funcionamiento de servidores
- Disponibilidad de sistemas críticos

El análisis combinado de estas variables podrá generar alertas. Por ejemplo:

RD Propone RD Propone

Una pérdida simultánea de cámara / apertura de acceso / anomalía eléctrica, deberá producir una alerta de prioridad superior a cualquiera de esos eventos considerados individualmente.

12. Centro de Control del Establecimiento

Cada establecimiento deberá disponer de un centro de control donde converjan las principales señales de seguridad. El operador autorizado deberá poder visualizar:

- Cámaras
- Alarmas
- Controles de acceso
- Detecciones
- Incidencias
- Estado de sistemas
- Comunicaciones institucionales
- Equipos críticos

Las acciones ejecutadas desde el centro deberán quedar registradas.

13. Centro Nacional de Monitoreo

Los centros de control locales deberán estar conectados con el Centro Nacional de Monitoreo, Inteligencia y Análisis Penitenciario establecido en el Capítulo IX. El centro nacional deberá permitir:

- Observar tendencias
- Comparar establecimientos
- Identificar patrones
- Detectar fallas recurrentes
- Coordinar incidentes
- Supervisar disponibilidad tecnológica
- Emitir alertas nacionales
- Apoyar investigaciones

No deberá sustituir al mando local. Su función será proporcionar una segunda capa de supervisión y análisis.

14. Inteligencia artificial como herramienta auxiliar

RD Propone RD Propone

La inteligencia artificial podrá utilizarse para analizar grandes volúmenes de información y detectar anomalías que puedan pasar inadvertidas durante una supervisión exclusivamente humana.

Podrá utilizarse para identificar:

- Patrones inusuales de acceso
- Repetición de incidentes
- Horarios de mayor riesgo
- Zonas donde se concentran eventos
- Fallas tecnológicas recurrentes
- Comportamientos operativos anómalos
- Relaciones entre distintos incidentes

La inteligencia artificial deberá actuar como herramienta de apoyo.

Ninguna decisión disciplinaria, penal o que afecte derechos fundamentales deberá basarse exclusivamente en una alerta algorítmica. Toda alerta deberá ser revisada por personal autorizado.

15. Sistema de alertas por niveles

Las alertas deberán clasificarse por niveles.

Nivel 1 Técnico	Fallas de equipos o infraestructura sin indicios inmediatos de actividad ilícita.
Nivel 2 Seguridad	Eventos que puedan representar una vulnerabilidad.
Nivel 3 — Incidente	Detección de un dispositivo no autorizado, manipulación de un sistema o violación de un control.
Nivel 4 — Crítico	Incidente con indicios de coordinación criminal, participación interna organizada, ataque contra infraestructura o riesgo inmediato para la seguridad.

Cada nivel deberá tener un protocolo de respuesta definido.

16. Tiempo máximo de respuesta

El sistema deberá establecer indicadores de tiempo para:

- Detección

RD Propone RD Propone

- Reconocimiento
- Confirmación
- Desplazamiento del personal
- Intervención
- Preservación de evidencia
- Elaboración del informe

La evaluación del establecimiento deberá considerar no solamente cuántos incidentes ocurrieron, sino qué tan rápido y eficazmente respondió.

17. Sistema de control de acceso

El ingreso de personal, visitantes, proveedores, contratistas, vehículos, mercancías, deberá estar registrado electrónicamente. El sistema deberá permitir conocer:

- Quién ingresó
- Cuándo ingresó
- Por qué acceso
- Cuándo salió
- Con qué autorización
- En qué área estuvo autorizado a permanecer

En áreas críticas deberán establecerse controles adicionales.

18. Integración de cámaras y acceso

Una de las principales ventajas del sistema será la posibilidad de correlacionar registros. Ejemplo:

Una persona ingresa al establecimiento a las 9:00 a. m.; pasa por determinado punto; accede a un área específica; ocurre una detección de dispositivo a las 9:18 a. m.; posteriormente abandona el área.

El sistema deberá permitir reconstruir esa secuencia para apoyar la investigación. Esto transforma una grabación aislada en una *línea de tiempo investigativa*.

19. Control tecnológico de visitantes y proveedores

Los visitantes y proveedores deberán atravesar controles proporcionales al nivel de riesgo. La tecnología podrá incluir, según corresponda:

- Inspección electrónica
- Detección de objetos

RD Propone RD Propone

- Controles de identidad
- Validación de autorización
- Registro de ingreso y salida
- Videovigilancia
- Trazabilidad de mercancías

La selección de tecnologías deberá realizarse mediante evaluación técnica y de costo-beneficio.

20. Sistema de trazabilidad de mercancías

Toda mercancía que ingrese a un establecimiento deberá estar asociada, cuando corresponda, a:

- Proveedor
- Vehículo
- Conductor
- Funcionario receptor
- Fecha
- Hora
- Tipo de mercancía
- Cantidad
- Area de destino

Las entregas deberán poder reconstruirse posteriormente. Esto permitirá investigar no solamente qué fue encontrado, sino por qué vía pudo haber ingresado.

21. Zona tecnológica segura

Cada establecimiento deberá disponer de una sala técnica protegida donde se encuentren los componentes críticos del sistema.

El acceso deberá estar restringido y registrado.

Los equipos críticos deberán contar, cuando corresponda, con:

- Energía de respaldo
- Protección contra variaciones eléctricas
- Climatización adecuada
- Sistemas contra incendios
- Control de acceso

RD Propone RD Propone

- Monitoreo
- Redundancia

22. Continuidad operacional

La seguridad no podrá depender exclusivamente de la electricidad comercial o de una conexión de internet. Los sistemas críticos deberán disponer de mecanismos de continuidad. Como mínimo deberán evaluarse:

- UPS;
- Generadores;
- Enlaces redundantes;
- Almacenamiento redundante;
- Respaldos;
- Procedimientos manuales de contingencia.

Una interrupción tecnológica no deberá significar una interrupción de la seguridad.

23. Ciberseguridad penitenciaria

Todos los sistemas deberán estar protegidos frente a:

- Accesos no autorizados
- Modificación de registros
- Robo de credenciales
- Malware
- Sabotaje digital
- Extracción de información
- Manipulación de cámaras
- Alteración de registros

Los sistemas de seguridad penitenciaria deberán mantenerse separados de redes que no necesiten acceso a ellos. Los privilegios de cada usuario deberán limitarse a sus funciones.

24. Identidad digital de operadores

Cada funcionario que utilice los sistemas tecnológicos deberá contar con una identidad digital individual. Quedará prohibido compartir credenciales.

El sistema deberá registrar:

- Usuario;

RD Propone RD Propone

- Fecha;
- Hora;
- Equipo utilizado;
- Operación realizada.

Esto permitirá establecer responsabilidad individual sobre las acciones realizadas dentro del sistema.

25. Redundancia

Los sistemas críticos deberán diseñarse bajo el principio de redundancia. Una falla en una cámara, un servidor, un enlace, una fuente de energía, un sensor, un sistema de almacenamiento, no deberá eliminar completamente la capacidad de vigilancia. La redundancia deberá determinarse según el nivel de criticidad.

26. Pruebas de seguridad

La tecnología instalada deberá someterse periódicamente a pruebas controladas. Estas podrán incluir:

- Pruebas de detección;
- Pruebas de cámaras;
- Pruebas de alarmas;
- Pruebas de continuidad;
- Pruebas de respaldo;
- Pruebas de recuperación;
- Simulaciones de incidentes;
- Pruebas de control de acceso.

Las pruebas deberán realizarse de forma autorizada y documentada.

27. Prohibición de sistemas opacos

El Estado no deberá adquirir tecnologías cuya operación crítica dependa exclusivamente del conocimiento reservado del proveedor. Los contratos deberán exigir:

- Documentación técnica
- Capacitación
- Manuales
- Mecanismos de auditoría
- Acceso institucional a registros

RD Propone RD Propone

- Continuidad de soporte
- Mecanismos de sustitución del proveedor

La Administración deberá conservar capacidad real de supervisión.

28. Interoperabilidad

Los sistemas adquiridos deberán utilizar estándares que permitan, cuando resulte técnica y jurídicamente procedente, su integración con:

- Videovigilancia;
- Control de acceso;
- Sensores;
- Sistemas de alarmas;
- Centro de monitoreo;
- Sistemas de gestión penitenciaria.

Se deberá evitar crear múltiples plataformas aisladas que no puedan intercambiar información.

29. Protección de datos

La información obtenida mediante los sistemas de seguridad deberá manejarse bajo criterios de:

- Necesidad
- Finalidad
- Proporcionalidad
- Seguridad
- Acceso restringido
- Trazabilidad
- Conservación limitada conforme a la finalidad y la ley

El tratamiento de datos personales deberá ajustarse al marco jurídico aplicable, incluida la Ley 172-13.

30. Indicadores tecnológicos nacionales

Cada establecimiento deberá ser evaluado periódicamente mediante indicadores tales como:

- Porcentaje de cámaras operativas
- Tiempo promedio de reparación

RD Propone RD Propone

- Disponibilidad de sistemas críticos
- Cantidad de detecciones
- Cantidad de falsos positivos
- Tiempo promedio de respuesta
- Incidentes de manipulación
- Fallas de energía
- Fallas de comunicaciones
- Disponibilidad del almacenamiento
- Cumplimiento de mantenimiento

Esto permitirá pasar de una evaluación subjetiva a una evaluación basada en datos.

31. Semáforo tecnológico penitenciario

El sistema nacional podrá utilizar una clasificación operativa:

VERDE:	Sistemas disponibles y controles funcionando adecuadamente.
AMARILLO:	Vulnerabilidades o fallas que requieren corrección.
ROJO:	Vulnerabilidad crítica que compromete significativamente la seguridad.

El indicador deberá utilizarse para orientar recursos y acciones correctivas, no como mecanismo de sanción automática.

32. Implementación por fases

La modernización tecnológica deberá ejecutarse gradualmente.

FASE I Diagnóstico

Inventario de:

- Cámaras
- Sensores
- Controles
- Redes
- Sistemas eléctricos
- Comunicaciones
- Infraestructura

RD Propone RD Propone

FASE II Centros prioritarios

- Implementación inicial en establecimientos con mayores niveles de riesgo.

FASE III Integración

- Conexión de los sistemas locales con el Centro Nacional de Monitoreo.

FASE IV Expansión

- Extensión al resto de los establecimientos.

FASE V Optimización

- Actualización tecnológica, análisis de resultados y sustitución de sistemas obsoletos.

33. Principio de neutralidad tecnológica

La legislación y las políticas públicas no deberán establecer una única tecnología obligatoria. Deberán establecerse:

- Resultados esperados
- Niveles mínimos de seguridad
- Estándares de disponibilidad
- Requisitos de interoperabilidad
- Requisitos de protección
- Indicadores de desempeño

De esta manera, el Estado podrá adquirir nuevas tecnologías sin tener que modificar permanentemente la legislación.

34. Principio de costo-eficiencia

La modernización no deberá convertirse en una carrera por adquirir la tecnología más costosa. Antes de cada adquisición deberá evaluarse:

- Problema que pretende resolver;
- Eficacia demostrada;
- Costo inicial;
- Costo de mantenimiento;
- Vida útil;

RD Propone RD Propone

- Disponibilidad de repuestos;
- Capacitación;
- Interoperabilidad;
- Riesgos;
- Posibilidad de ampliación.

El Estado deberá priorizar soluciones que puedan mantenerse durante toda su vida útil.

35. Resultado esperado

La arquitectura tecnológica propuesta deberá producir una transformación fundamental:

ANTES

Ingreso del dispositivo / Descubrimiento ocasional / Incautación / Investigación limitada

MODELO PROPUESTO

Prevención / Control de acceso / Detección / Localización / Alerta / Respuesta / Incautación / Preservación de evidencia / Análisis / Identificación de la cadena de suministro / Investigación / Sanción / Corrección de vulnerabilidad.

El objetivo final no será simplemente encontrar más teléfonos.

Será hacer progresivamente más difícil que un establecimiento penitenciario pueda ser utilizado como plataforma de coordinación criminal.

CAPÍTULO XIII
IMPLEMENTACIÓN, PRIORIZACIÓN, COSTOS Y CRONOGRAMA NACIONAL

1. Finalidad

La implementación del Sistema Nacional de Seguridad Tecnológica Penitenciaria deberá realizarse de manera gradual, priorizada y medible.

El Estado no deberá intentar instalar simultáneamente todos los componentes tecnológicos en todos los establecimientos.

La estrategia deberá comenzar por identificar los centros con mayores niveles de riesgo, corregir sus vulnerabilidades principales, medir los resultados y utilizar las lecciones obtenidas para ampliar progresivamente el sistema.

2. Principio de implementación progresiva

La modernización deberá desarrollarse bajo el principio:

RD Propone RD Propone

Primero controlar los riesgos críticos; después ampliar la cobertura.

La existencia de recursos limitados no deberá utilizarse como razón para posponer indefinidamente la modernización, por el contrario, deberá permitir establecer prioridades objetivas.

3. Fase 0 Diagnóstico nacional

Antes de realizar grandes adquisiciones deberá efectuarse un diagnóstico integral de todos los establecimientos. El diagnstico deberá determinar:

- Estado de las cámaras
- Cobertura de videovigilancia
- Controles de acceso
- Sistemas de detección
- Infraestructura eléctrica
- Sistemas de comunicaciones
- Redes
- Centros de control
- Disponibilidad de energía
- Sistemas de respaldo
- Personal disponible
- Procedimientos de inspección
- Historial de incidentes
- Existencia de vulnerabilidades físicas
- Contratos tecnológicos existentes
- Costos de mantenimiento
- Capacidad de respuesta

El resultado deberá ser un Mapa Nacional de Vulnerabilidades Penitenciarias.

4. Clasificación de establecimientos

Con base en el diagnóstico, los establecimientos podrán clasificarse en:

Categoría I Riesgo crítico

Centros que presentan múltiples vulnerabilidades simultáneas o incidentes de alta gravedad.

Categoría II Riesgo alto

RD Propone RD Propone

Centros con vulnerabilidades importantes que requieren intervención prioritaria.

Categoría III Riesgo moderado

Centros con controles funcionales pero con necesidades de modernización.

Categoría IV Riesgo controlado

Centros que cumplen los estándares mínimos y requieren principalmente mantenimiento y actualización. La clasificación deberá revisarse periódicamente.

5. Criterios de priorización

La prioridad de intervención no deberá determinarse únicamente por el tamaño del establecimiento. Deberán considerarse:

1. Número de personas privadas de libertad.
2. Historial de incidentes.
3. Nivel de riesgo de la población penitenciaria.
4. Evidencia de comunicaciones no autorizadas.
5. Vulnerabilidades físicas.
6. Capacidad tecnológica existente.
7. Condiciones del personal.
8. Ubicación.
9. Importancia estratégica.
10. Historial de fallas de seguridad.
11. Nivel de exposición a corrupción o infiltración.
12. Capacidad de respuesta ante emergencias.

6. Fase I Contención inmediata

Durante la primera etapa deberán ejecutarse medidas de bajo y mediano costo que produzcan resultados rápidos. Entre ellas:

- Reparación de cámaras existentes
- Eliminación de puntos ciegos
- Revisión de controles de acceso
- Inventario tecnológico
- Revisión de procedimientos
- Inspecciones extraordinarias
- Control de llaves

RD Propone RD Propone

- Identificación de áreas vulnerables
- Fortalecimiento de registros
- Creación de protocolos
- Capacitación del personal
- Establecimiento de indicadores
- Preservación de evidencias
- Creación de canales confidenciales de denuncia

Esta etapa deberá demostrar que el programa no depende exclusivamente de nuevas adquisiciones.

7. Fase II Centros piloto

Se seleccionará un número limitado de establecimientos para implementar integralmente el modelo. Los centros piloto deberán permitir probar:

- Videovigilancia
- Detección de dispositivos
- Control de acceso
- Centro de control
- Sistemas de respaldo
- Monitoreo
- Protocolos de respuesta
- Comunicaciones institucionales
- Integración de datos

La selección deberá realizarse con criterios técnicos y no únicamente administrativos.

8. Evaluación de los pilotos

Los pilotos deberán evaluarse antes de proceder a una expansión nacional. Deberán medirse:

- Incidentes antes y después
- Tiempo de detección
- Tiempo de respuesta
- Disponibilidad tecnológica
- Falsos positivos
- Fallas técnicas
- Costo de operación

RD Propone RD Propone

- Mantenimiento
- Aceptación del personal
- Necesidades de capacitación
- Vulnerabilidades no previstas

No deberá ampliarse una tecnología simplemente porque fue adquirida. Deberá ampliarse cuando haya demostrado utilidad bajo condiciones reales.

9. Fase III Expansión priorizada

Una vez evaluados los pilotos, la implementación deberá extenderse primero a los establecimientos de mayor riesgo. La expansión podrá realizarse por grupos. Cada grupo deberá completar:

Diagnóstico / Instalación capacitación / Prueba / Certificación / Operación / Auditoría

10. Fase IV Cobertura nacional

La cuarta etapa tendrá como objetivo alcanzar todos los establecimientos penitenciarios que requieran los componentes del sistema. Los centros de menor riesgo podrán requerir soluciones más sencillas. El principio deberá ser:

La tecnología deberá corresponder al riesgo.

No todos los establecimientos necesitan exactamente el mismo equipamiento.

11. Fase V Modernización permanente

La implementación no finalizará con la instalación. Deberá existir un programa permanente de:

- Mantenimiento
- Actualización
- Sustitución
- Capacitación
- Auditoría
- Pruebas
- Evaluación
- Renovación tecnológica

Todo sistema tecnológico tiene una vida útil limitada.

Por ello, el presupuesto deberá contemplar el ciclo completo del sistema.

RD Propone RD Propone

12. Modelo de presupuesto

El presupuesto deberá dividirse en cinco grandes categorías:

A. Inversión inicial

- Cámaras
- Sensores
- Sistemas de detección
- Servidores
- Redes
- Almacenamiento
- Centros de control
- Sistemas de respaldo
- Controles de acceso

B. Infraestructura

- Cableado;
- Energía;
- Protección eléctrica;
- Climatización;
- Adecuaciones físicas;
- Espacios técnicos.

C. Software y licencias

- Plataformas;
- Administración;
- Analítica;
- Monitoreo;
- Ciberseguridad;
- Almacenamiento.

D. Recursos humanos

- Capacitación;
- Especialistas;
- Operadores;
- Técnicos;
- Auditoría.

RD Propone RD Propone

E. Operación y mantenimiento

- Repuestos;
- Soporte;
- Actualizaciones;
- Mantenimiento preventivo;
- Mantenimiento correctivo;
- Renovación.

13. Costo total de propiedad

Las adquisiciones deberán evaluarse utilizando el concepto de:

Costo Total de Propiedad - TCO (Total Cost of Ownership).

No deberá considerarse únicamente el precio de compra.

Una solución económica que requiere mantenimiento excesivamente costoso puede resultar más onerosa que una solución de mayor inversión inicial pero menor costo operativo. La evaluación deberá considerar un horizonte plurianual.

14. Prohibición de adquisiciones fragmentadas sin integración

Las instituciones deberán evitar adquirir cámaras de un proveedor, sensores de otro, controles de acceso de otro, plataformas independientes, sistemas incompatibles, cuando ello impida posteriormente integrar la información. La compra deberá considerar desde el principio la arquitectura nacional.

15. Compras basadas en resultados

Las contrataciones deberán establecer requisitos funcionales, por ejemplo, en lugar de establecer únicamente *"adquirir X cámaras"*, deberá establecerse:

"garantizar cobertura continua de las áreas críticas, disponibilidad mínima determinada y generación de alertas ante pérdida de señal".

El proveedor deberá responder por el resultado contratado.

16. Contratos con indicadores de desempeño

Los contratos tecnológicos deberán incorporar indicadores verificables. Entre ellos:

- Disponibilidad;
- Tiempo de respuesta;

RD Propone RD Propone

- Tiempo de reparación;
- Porcentaje de equipos funcionales;
- Seguridad de la información;
- Actualización;
- Soporte;
- Cumplimiento de mantenimiento.

Cuando legalmente sea viable, parte del pago deberá estar vinculado al cumplimiento de niveles de servicio previamente establecidos.

17. Evitar dependencia tecnológica

Los contratos deberán establecer mecanismos para evitar que el Estado quede atrapado en un único proveedor. Deberán considerarse:

- Estándares abiertos
- Documentación
- Capacitación
- Transferencia de conocimiento
- Acceso institucional a la información
- Portabilidad de datos
- Interoperabilidad
- Disponibilidad de repuestos
- Mecanismos de transición

18. Aprovechamiento de infraestructura existente

Antes de reemplazar cualquier sistema deberán evaluarse los equipos existentes. Un equipo podrá:

1. Mantenerse
2. Repararse
3. Actualizarse
4. Integrarse
5. Trasladarse a una zona de menor criticidad
6. Sustituirse

La decisión deberá basarse en costo, seguridad y vida útil.

19. Fondo de mantenimiento tecnológico

RD Propone RD Propone

Deberá establecerse una partida presupuestaria permanente destinada al mantenimiento de los sistemas. La experiencia demuestra que instalar equipos sin garantizar mantenimiento produce progresivamente:

- Cámaras apagadas;
- Sensores fuera de servicio;
- Sistemas obsoletos;
- Servidores sin capacidad;
- Baterías agotadas;
- Redes deterioradas.

Por ello el mantenimiento deberá formar parte del proyecto desde el primer día.

20. Presupuesto plurianual

El programa deberá estructurarse mediante una planificación presupuestaria plurianual. Esto permitirá separar:

Año 1	Diagnóstico, pilotos y correcciones críticas.
Año 2	Expansión hacia establecimientos prioritarios.
Año 3	Ampliación de cobertura e integración nacional.
Año 4	Optimización, auditoría y modernización.
Año 5	Evaluación integral y renovación de tecnologías que hayan alcanzado su ciclo operativo.

El calendario definitivo deberá ajustarse a la disponibilidad presupuestaria y a los resultados de las fases anteriores.

21. Equipo nacional de implementación

Deberá existir una unidad técnica responsable de coordinar la ejecución, esta deberá integrar, según corresponda:

- Autoridades penitenciarias
- Especialistas tecnológicos
- Especialistas en telecomunicaciones
- Expertos en seguridad
- Especialistas jurídicos
- Personal de infraestructura

RD Propone RD Propone

- Especialistas en ciberseguridad
- Responsables presupuestarios

Su función será coordinar, no sustituir las competencias legales de cada institución.

22. Capacitación antes de la puesta en funcionamiento

Ningún sistema deberá ponerse en operación definitiva sin que los funcionarios responsables hayan recibido capacitación. La capacitación deberá abarcar:

- Operación;
- Seguridad;
- Respuesta ante alertas;
- Preservación de evidencia;
- Protección de datos;
- Ciberseguridad;
- Mantenimiento básico;
- Procedimientos de contingencia.

23. Certificación de cada establecimiento

Antes de declarar operativo un sistema deberá realizarse una certificación. La certificación deberá verificar:

- Funcionamiento de cámaras
- Detección
- Alarmas
- Comunicaciones
- Energía
- Respaldo
- Almacenamiento
- Controles de acceso
- Conectividad
- Procedimientos
- Capacitación

Un establecimiento que no cumpla los requisitos mínimos deberá permanecer en condición de implementación hasta corregir las deficiencias.

24. Tablero nacional de ejecución

El programa deberá contar con un tablero de seguimiento que permita conocer:

RD Propone RD Propone

- Establecimientos diagnosticados;
- Establecimientos intervenidos;
- Establecimientos certificados;
- Porcentaje de cobertura;
- Porcentaje de equipos funcionales;
- Presupuesto ejecutado;
- Incidentes registrados;
- Tiempo de respuesta;
- Fallas pendientes.

El tablero deberá permitir identificar rápidamente dónde existen retrasos.

25. Transparencia

El Estado deberá publicar periódicamente información agregada sobre:

- Avance del programa
- Inversión realizada
- Número de establecimientos incorporados
- Principales indicadores
- Incidentes
- Resultados de auditorías

La publicación deberá proteger información cuya divulgación pueda comprometer la seguridad penitenciaria. La transparencia no deberá significar revelar:

- Ubicación exacta de sensores;
- Puntos vulnerables;
- Configuraciones de seguridad;
- Credenciales;
- Protocolos operativos sensibles.

26. Evaluación independiente

Al menos periódicamente deberá realizarse una evaluación independiente del programa. La evaluación deberá determinar:

- Si se cumplieron los objetivos
- Si los sistemas funcionan
- Si los recursos fueron utilizados eficientemente
- Si existen fallas estructurales

RD Propone RD Propone

- Si los indicadores mejoraron
- Qué modificaciones son necesarias

La evaluación deberá estar separada de la unidad directamente responsable de la ejecución.

27. Mecanismo de corrección

Cuando una evaluación determine una falla significativa, deberá establecerse:

1. Descripción del problema
2. Nivel de riesgo
3. Responsable
4. Medida correctiva
5. Plazo
6. Presupuesto
7. Verificación
8. Cierre de la incidencia

No deberá considerarse concluida una vulnerabilidad simplemente porque se haya emitido un informe.

28. Cronograma de referencia

El programa nacional podrá organizarse inicialmente de la siguiente manera:

Etapa	Periodo	Objetivo
Diagnóstico nacional	0–6 meses	Identificar vulnerabilidades
Contención inmediata	0–6 meses	Corregir fallas críticas
Centros piloto	6–12 meses	Probar arquitectura
Evaluación	12–15 meses	Medir resultados
Primera expansión	15–24 meses	Intervenir centros prioritarios
Segunda expansión	24–36 meses	Ampliar cobertura
Cobertura nacional	36–48 meses	Completar implementación
Optimización	48–60 meses	Evaluación y renovación

RD Propone RD Propone

Este cronograma deberá considerarse referencial y podrá modificarse conforme a los resultados y a la disponibilidad presupuestaria.

29. Regla de no expansión automática

El Gobierno no deberá comprometerse a comprar tecnología para todos los establecimientos simplemente porque un programa piloto haya sido contratado. Antes de cada etapa de expansión deberá verificarse:

- Eficacia
- Costo
- Disponibilidad
- Mantenimiento
- Resultados
- Seguridad
- Aceptación operacional

30. Indicadores de éxito

El programa deberá ser evaluado mediante resultados. Entre los indicadores principales estarán:

- Reducción de dispositivos no autorizados detectados
- Reducción de intentos de introducción
- Reducción del tiempo de detección
- Reducción del tiempo de respuesta
- Incremento de incidentes correctamente investigados
- Reducción de fallas tecnológicas
- Incremento de disponibilidad de sistemas
- Reducción de puntos ciegos
- Aumento de cumplimiento de protocolos
- Identificación de redes de suministro

La reducción de dispositivos encontrados no deberá interpretarse automáticamente como éxito.

Una disminución puede significar menor ingreso de dispositivos, pero también podría significar menor capacidad de detección.

Por eso deberán analizarse múltiples indicadores simultáneamente.

RD Propone RD Propone

31. Evaluación de impacto

Después de los primeros 24 meses deberá realizarse una evaluación nacional del programa. Esta evaluación deberá responder:

1. ¿Se redujo el ingreso de dispositivos?
2. ¿Se redujo su utilización?
3. ¿Disminuyeron las comunicaciones ilícitas?
4. ¿Se redujeron incidentes vinculados a coordinación criminal desde los centros?
5. ¿Aumentó la capacidad de investigación?
6. ¿Se redujeron vulnerabilidades internas?
7. ¿Los sistemas tecnológicos permanecen operativos?
8. ¿El costo de operación es sostenible?

Las respuestas deberán determinar la siguiente etapa del programa.

32. Principio de sostenibilidad

El sistema solamente podrá considerarse exitoso si puede mantenerse financieramente y operativamente durante el tiempo. Por ello, el proyecto deberá contemplar desde el inicio:

- Presupuesto de mantenimiento
- Sustitución tecnológica
- Capacitación continua
- Actualización
- Auditoría
- Renovación de infraestructura
- Ciberseguridad

33. Resultado esperado

Al finalizar la implementación nacional deberá existir un sistema penitenciario en el que los puntos de acceso estén controlados, las áreas críticas sean observables, los dispositivos no autorizados puedan ser detectados, las alertas lleguen a operadores responsables, los incidentes sean documentados, la evidencia pueda preservarse, los sistemas puedan auditarse, las fallas sean identificadas, los responsables puedan ser investigados, los recursos públicos puedan ser evaluados.

La modernización tecnológica deberá convertirse así en una capacidad permanente del Estado y no en un proyecto temporal.

RD Propone RD Propone

34. Principio final de implementación

El programa deberá seguir una regla sencilla:

No comprar primero y preguntar después qué problema se pretendía resolver.

Primero deberá identificarse la vulnerabilidad / Después deberá determinarse la solución / Luego deberá probarse / Posteriormente deberá medirse / Y solamente entonces deberá ampliarse.

La seguridad penitenciaria deberá construirse mediante evidencia, tecnología apropiada, disciplina institucional y evaluación permanente.

CAPÍTULO XIV
SISTEMA NACIONAL DE INDICADORES, METAS Y EVALUACIÓN DE RESULTADOS

1. Objeto

El Sistema Nacional de Indicadores y Evaluación de Resultados tendrá como finalidad medir de manera permanente la eficacia, eficiencia, disponibilidad, seguridad y sostenibilidad del Sistema Nacional de Seguridad Tecnológica Penitenciaria.

La existencia de equipos, contratos, instalaciones o inversiones no será considerada por sí misma evidencia de éxito. La evaluación deberá concentrarse en los resultados obtenidos.

2. Principio de medición objetiva

Toda institución responsable deberá utilizar indicadores verificables. Los indicadores deberán ser:

- Medibles
- Comparables
- Periódicos
- Auditables
- Verificables
- Suficientemente claros para permitir su interpretación

Cuando sea posible, los resultados deberán compararse con una línea base anterior a la implementación.

3. Línea base nacional

RD Propone RD Propone

Antes de la implementación deberá establecerse una línea base nacional. Esta deberá incluir, como mínimo:

- Cantidad de dispositivos no autorizados incautados
- Intentos de introducción registrados
- Incidentes de comunicaciones clandestinas
- Puntos ciegos identificados
- Cámaras operativas
- Cámaras fuera de servicio
- Disponibilidad de sistemas
- Tiempo de respuesta
- Cantidad de investigaciones
- Participación interna detectada
- Participación externa detectada
- Incidentes relacionados con coordinación criminal desde centros penitenciarios

Sin una línea base no será posible determinar adecuadamente el impacto de la reforma.

4. Indicadores de prevención

Se establecerán indicadores destinados a medir la capacidad preventiva, entre ellos:

1. Número de intentos de introducción detectados.
2. Porcentaje de controles de acceso realizados conforme al protocolo.
3. Porcentaje de visitantes sometidos al procedimiento correspondiente.
4. Porcentaje de proveedores registrados.
5. Incidentes relacionados con violaciones de protocolos.
6. Reincidencia de personas involucradas en intentos de introducción.

5. Indicadores de detección

Se medirán:

- Número de dispositivos detectados
- Tiempo promedio entre activación y detección
- Porcentaje de eventos correctamente identificados
- Porcentaje de falsos positivos
- Cobertura de las zonas críticas
- Disponibilidad de los sistemas de detección

La evolución de estos indicadores deberá interpretarse conjuntamente.

RD Propone RD Propone

6. Indicadores de localización

Cuando la tecnología lo permita, deberán medirse:

- Porcentaje de detecciones con ubicación aproximada
- Tiempo promedio para determinar la zona
- Precisión operacional
- Porcentaje de incidentes en los que fue posible identificar el área de origen

La capacidad de localizar deberá evaluarse separadamente de la capacidad de detectar.

7. Indicadores de respuesta

Se medirán:

T1-Tiempo de detección	Desde la aparición del evento hasta la generación de la alerta.
T2 - Tiempo de reconocimiento	Desde la alerta hasta su validación por el operador.
T3 - Tiempo de intervención	Desde la confirmación hasta la llegada del personal autorizado.
T4 - Tiempo de aseguramiento	Desde la intervención hasta el control de la situación.
T5 - Tiempo de documentación	Desde el incidente hasta la elaboración del registro correspondiente.

Estos tiempos deberán registrarse automáticamente cuando la infraestructura tecnológica lo permita.

8. Indicadores de investigación

Deberán medirse:

- Incidentes investigados
- Incidentes con identificación del dispositivo
- Incidentes con identificación del usuario
- Incidentes con identificación del mecanismo de ingreso
- Investigaciones que identificaron participación externa
- Investigaciones que identificaron participación interna

RD Propone RD Propone

- Investigaciones remitidas al Ministerio Público
- Investigaciones concluidas

9. Indicadores de cadena de suministro

Uno de los objetivos principales del programa será dejar de limitarse a confiscar dispositivos y comenzar a identificar cómo ingresaron. Por ello deberán medirse:

- Dispositivos cuyo origen pudo determinarse
- Casos en que se identificó al facilitador
- Casos en que se identificó al introductor
- Casos en que se identificó al financiador
- Casos con participación de personal
- Casos con participación de visitantes
- Casos relacionados con proveedores
- Redes de suministro identificadas

10. Indicadores de seguridad tecnológica

Cada establecimiento deberá medir:

- Porcentaje de cámaras operativas;
- Porcentaje de sensores operativos;
- Disponibilidad de servidores;
- Disponibilidad de almacenamiento;
- Disponibilidad de energía de respaldo;
- Disponibilidad de comunicaciones;
- Cantidad de fallas;
- Tiempo promedio de reparación;
- Incidentes de manipulación;
- Intentos de acceso no autorizado.

11. Indicadores de integridad institucional

Deberán registrarse:

- Denuncias recibidas
- Denuncias investigadas
- Investigaciones internas
- Funcionarios involucrados
- Funcionarios sancionados conforme al debido proceso

RD Propone RD Propone

- Casos remitidos al Ministerio Público
- Incidentes relacionados con corrupción
- Reincidencia institucional

La publicación de estos indicadores deberá respetar las restricciones legales sobre datos personales y procesos en curso.

12. Indicadores de capacitación

Deberán medirse:

- Porcentaje del personal capacitado
- Horas de capacitación
- Porcentaje aprobado en evaluaciones
- Simulacros realizados
- Tiempo de respuesta durante simulacros
- Personal certificado
- Personal que requiere capacitación adicional

La capacitación no deberá medirse únicamente por número de asistentes.

13. Indicadores de mantenimiento

Deberán registrarse:

- Mantenimiento preventivo realizado
- Mantenimiento pendiente
- Tiempo de reparación
- Equipos fuera de servicio
- Reincidencia de fallas
- Costos de mantenimiento
- Cumplimiento de contratos
- Cumplimiento de niveles de servicio

14. Indicadores presupuestarios

El programa deberá medir:

- Presupuesto aprobado
- Presupuesto comprometido
- Presupuesto ejecutado
- Costo por establecimiento

RD Propone RD Propone

- Costo de mantenimiento
- Costo por sistema
- Desviaciones presupuestarias
- Ahorros derivados del aprovechamiento de infraestructura existente

15. Indicadores de eficacia

Los indicadores de eficacia deberán responder a la pregunta:

¿Está funcionando el sistema?

Entre ellos podrán incluirse:

- Variación de los intentos de introducción
- Variación de las comunicaciones no autorizadas detectadas
- Tiempo de detección
- Tiempo de respuesta
- Capacidad de identificar responsables
- Reincidencia
- Cantidad de incidentes relacionados con coordinación criminal

Estos indicadores deberán interpretarse conjuntamente y nunca de manera aislada.

16. Indicadores de eficiencia

La eficiencia deberá responder:

¿Estamos obteniendo resultados razonables en relación con los recursos utilizados?

Se deberán analizar:

- Costo por establecimiento
- Costo de mantenimiento
- Costo por incidente atendido
- Disponibilidad tecnológica
- Vida útil de los equipos
- Horas de operación
- Costos de sustitución

17. Indicadores de sostenibilidad

Un sistema no deberá considerarse exitoso si funciona durante un año y posteriormente queda abandonado. Deberán evaluarse:

RD Propone RD Propone

- Capacidad presupuestaria
- Mantenimiento
- Disponibilidad de repuestos
- Actualización
- Capacitación
- Renovación
- Dependencia de proveedores
- Obsolescencia tecnológica

18. Indicadores de calidad de datos

El Centro Nacional deberá evaluar la calidad de la información utilizada, determinando:

- Si los datos están completos
- Si son consistentes
- Si están actualizados
- Si pueden ser auditados
- Si existen duplicidades
- Si existen registros contradictorios
- Si las fuentes están correctamente identificadas

Una política basada en datos deficientes puede producir decisiones equivocadas.

19. Tablero Nacional de Seguridad Penitenciaria

El tablero deberá permitir visualizar, según los permisos correspondientes:

- Situación de cada establecimiento
- Incidentes
- Disponibilidad tecnológica
- Tiempos de respuesta
- Vulnerabilidades
- Mantenimiento
- Cumplimiento
- Evolución de indicadores

El sistema deberá generar alertas cuando un indicador supere los límites establecidos.

20. Indicadores de alerta

Cada indicador crítico deberá contar con niveles de referencia. Por ejemplo:

RD Propone RD Propone

Normal	El comportamiento se encuentra dentro de los parámetros establecidos.
Advertencia	Existe una desviación que requiere análisis.
Crítico	Existe una desviación que requiere intervención inmediata.

Los umbrales deberán definirse técnicamente y revisarse periódicamente.

21. Metas nacionales

Las metas deberán establecerse utilizando la línea base. `No deberán fijarse objetivos arbitrarios sin considerar:

- Situación inicial
- Características del establecimiento
- Recursos disponibles
- Tecnología
- Riesgos
- Capacidad institucional

Las metas deberán poder revisarse cuando exista evidencia suficiente para demostrar que requieren modificación.

22. Metas diferenciadas por establecimiento

No todos los centros deberán tener necesariamente los mismos objetivos. Un establecimiento de máxima seguridad podrá requerir estándares tecnológicos superiores a uno de menor riesgo. Por ello deberán establecerse:

- Estándares nacionales mínimos
- Estándares adicionales según categoría de riesgo

23. Evaluación trimestral

Cada establecimiento deberá realizar una evaluación trimestral. El informe deberá contener:

- Indicadores
- Incidentes
- Fallas
- Acciones correctivas
- Mantenimiento

RD Propone RD Propone

- Capacitación
- Cumplimiento
- Recomendaciones

24. Evaluación semestral

Deberá identificar:

- Establecimientos con deterioro;
- Vulnerabilidades recurrentes;
- Tecnologías con bajo desempeño;
- Problemas presupuestarios;
- Necesidades de capacitación;
- Riesgos emergentes.

25. Informe anual nacional

El informe deberá presentar información agregada sobre:

- Evolución de incidentes
- Resultados
- Inversión
- Disponibilidad tecnológica
- Investigaciones
- Sanciones
- Mantenimiento
- Cumplimiento
- Vulnerabilidades
- Medidas correctivas

La información sensible deberá protegerse.

26. Auditoría de los indicadores

Los indicadores deberán ser auditables. Las instituciones no deberán poder modificar retrospectivamente los resultados sin dejar evidencia de:

- Quién realizó el cambio
- Cuándo
- Por qué
- Cuál era el dato original
- Cuál fue el dato corregido

RD Propone RD Propone

27. Prevención de manipulación estadística

La reducción de incidentes reportados no deberá interpretarse automáticamente como una mejora. El sistema deberá comparar:

- Incidentes registrados
- Detecciones tecnológicas
- Inspecciones
- Investigaciones
- Reportes internos
- Fallas de los sistemas

Una caída abrupta de reportes acompañada por una disminución de inspecciones o fallas tecnológicas deberá generar una alerta analítica.

28. Evaluación externa

Periódicamente deberá contratarse o designarse una entidad independiente con capacidad técnica para revisar:

- Metodología
- Indicadores
- Datos
- Resultados
- Sistemas
- Cumplimiento

La evaluación externa deberá producir recomendaciones públicas en la medida compatible con la seguridad.

29. Revisión de metas

Las metas deberán revisarse cuando:

- Aparezcan nuevas tecnologías
- Cambien los patrones delictivos
- Cambien las modalidades de introducción
- Exista evidencia de que una medida no funciona
- Cambie sustancialmente la infraestructura
- Aparezcan nuevos riesgos

La política deberá poder adaptarse.

RD Propone RD Propone

30. Sistema de aprendizaje institucional

Cada incidente relevante deberá producir una revisión posterior, esta deberá responder:

1. ¿Qué ocurrió?
2. ¿Cómo ocurrió?
3. ¿Por qué ocurrió?
4. ¿Qué controles fallaron?
5. ¿Qué controles funcionaron?
6. ¿Qué información estaba disponible?
7. ¿Qué información faltó?
8. ¿Qué medida debe modificarse?
9. ¿Quién debe ejecutar la corrección?
10. ¿Cuándo debe verificarse?

La finalidad no será únicamente determinar culpabilidades, también será *evitar que el mismo problema vuelva a producirse.*

31. Banco Nacional de Lecciones Aprendidas

Los incidentes relevantes deberán alimentar un banco nacional de lecciones aprendidas, el que podrá clasificar:

- Modalidad de ingreso
- Modalidad de ocultamiento
- Tecnología utilizada
- Vulnerabilidad aprovechada
- Respuesta
- Resultado
- Medida correctiva

La información deberá utilizarse para actualizar procedimientos en otros establecimientos.

32. Indicador de madurez institucional

Además de los indicadores individuales, cada establecimiento podrá recibir una evaluación de madurez basada en:

- Prevención
- Detección

RD Propone RD Propone

- Respuesta
- Investigación
- Tecnología
- Mantenimiento
- Capacitación
- Integridad
- Auditoría

El resultado deberá utilizarse para determinar prioridades de mejora. No deberá utilizarse como sustituto de investigaciones disciplinarias o penales.

33. Transparencia y protección de la seguridad

La ciudadanía deberá poder conocer los resultados generales del programa, sin embargo, no deberán publicarse detalles que permitan identificar:

- Puntos vulnerables
- Ubicación exacta de sensores
- Procedimientos operativos sensibles
- Configuraciones tecnológicas
- Mecanismos de respuesta que puedan ser explotados

La transparencia deberá coexistir con la seguridad operacional

34. Meta fundamental del sistema

El éxito del programa no deberá definirse por la cantidad de tecnología instalada.

La meta fundamental será *reducir progresivamente la capacidad de utilizar los establecimientos penitenciarios como centros de comunicación y coordinación para actividades ilícitas.*

La tecnología será el medio, la seguridad y la reducción del riesgo serán el resultado buscado.

35. Principio final de evaluación

El sistema deberá responder permanentemente cinco preguntas:

- ¿Qué está ocurriendo?
- ¿Por qué está ocurriendo?
- ¿Dónde está ocurriendo?
- ¿Qué estamos haciendo al respecto?
- ¿Está funcionando?

RD Propone RD Propone

Si la institución no puede responder estas cinco preguntas mediante información verificable, el sistema de seguridad deberá considerarse incompleto.

CAPÍTULO XV
GOBERNANZA Y COORDINACIÓN INTERINSTITUCIONAL DEL SISTEMA NACIONAL DE SEGURIDAD PENITENCIARIA

1. Objeto

El Sistema Nacional de Seguridad Penitenciaria deberá contar con una estructura institucional claramente definida que establezca:

- Quién dirige
- Quién ejecuta
- Quién supervisa
- Quién investiga
- Quién regula
- Quién audita
- Quién responde ante una falla

La coordinación institucional deberá evitar duplicidades y, especialmente, vacíos de responsabilidad.

2. Principio de rectoría

El Ministerio de Justicia deberá ejercer la rectoría administrativa y de política pública que corresponda al Sistema Penitenciario y Correccional, conforme al marco jurídico vigente.

La rectoría no deberá significar que todas las funciones sean ejecutadas directamente por el Ministerio. Cada institución deberá conservar las competencias que legalmente le correspondan.

3. Dirección General de Servicios Penitenciarios y Correccionales

La Dirección General de Servicios Penitenciarios y Correccionales constituirá el principal órgano operativo del sistema penitenciario.

Corresponderá a la Dirección, dentro de sus competencias:

- Ejecutar las políticas penitenciarias;
- Administrar los establecimientos;
- Implementar los protocolos;
- Supervisar al personal;

RD Propone RD Propone

- Ejecutar los controles;
- Administrar los centros de monitoreo;
- Coordinar la respuesta a incidentes;
- Mantener los registros operativos;
- Garantizar el cumplimiento de los procedimientos.

La Dirección deberá contar con capacidad técnica suficiente para operar el sistema tecnológico.

4. Ministerio de Justicia

Corresponderá al Ministerio de Justicia, conforme a sus competencias legales:

1. Formular y coordinar políticas públicas penitenciarias
2. Supervisar la implementación nacional
3. Coordinar las instituciones participantes
4. Promover las reformas normativas necesarias
5. Coordinar la planificación presupuestaria
6. Supervisar la ejecución general del programa
7. Presentar informes nacionales
8. Promover mecanismos de evaluación
9. Coordinar la cooperación nacional e internacional
10. Establecer estándares generales

El Ministerio no deberá sustituir las funciones operativas de la Dirección General.

5. Ministerio Público

El Ministerio Público conservará las competencias que le atribuya la Constitución y las leyes en materia de investigación y persecución penal.

Cuando una detección penitenciaria presente indicios de delito, deberá existir un mecanismo institucional que permita:

Detección / Preservación de evidencia / Comunicación / Investigación

El sistema penitenciario no deberá realizar por cuenta propia funciones que correspondan legalmente al Ministerio Público o a los órganos jurisdiccionales.

La Ley 80-25 contempla expresamente mecanismos de coordinación entre el Ministerio de Justicia y el procurador general para garantizar el acceso del Ministerio Público a las personas privadas de libertad cuando exista una investigación.

RD Propone RD Propone

6. Instituto Dominicano de las Telecomunicaciones

El INDOTEL deberá participar en los componentes relacionados con:

- Espectro radioeléctrico
- Telecomunicaciones
- Interferencias
- Soluciones técnicas de control
- Evaluación de tecnologías
- Coordinación con prestadoras
- Cumplimiento de la normativa sectorial

La Ley 153-98 constituye el marco general de las telecomunicaciones y atribuye al INDOTEL funciones regulatorias y de supervisión del sector.

7. Policía Nacional

La Policía Nacional podrá participar, conforme a sus competencias legales, en:

- Apoyo operativo
- Seguridad perimetral cuando corresponda
- Investigaciones coordinadas
- Análisis criminal
- Identificación de estructuras externas
- Apoyo ante incidentes de alto riesgo

Su participación deberá estar delimitada para evitar duplicidad con las funciones penitenciarias.

8. Poder Judicial

El Poder Judicial intervendrá dentro de sus competencias cuando las actuaciones requieran:

- Autorización judicial
- Control jurisdiccional
- Valoración de pruebas
- Imposición de sanciones judiciales
- Protección de garantías fundamentales

El sistema tecnológico deberá diseñarse respetando la separación de funciones entre administración penitenciaria, investigación y jurisdicción.

RD Propone RD Propone

9. Órganos de control

Los órganos de control del Estado deberán poder auditar, dentro de sus respectivas competencias:

- Utilización de recursos
- Contrataciones
- Cumplimiento de procedimientos
- Desempeño institucional
- Mantenimiento
- Adquisición de tecnología

Las auditorías deberán poder determinar tanto irregularidades financieras como deficiencias de gestión.

10. Unidad Nacional de Coordinación

Se propone crear una Unidad Nacional de Coordinación de Seguridad Tecnológica Penitenciaria, adscrita al Ministerio de Justicia. Esta unidad no sustituirá a la Dirección General de Servicios Penitenciarios y Correccionales.

Su función será asegurar que todas las piezas del sistema funcionen de manera coordinada.

11. Funciones de la Unidad Nacional de Coordinación

La unidad tendrá, entre otras, las siguientes funciones:

1. Coordinar la implementación nacional.
2. Dar seguimiento al cronograma.
3. Supervisar indicadores.
4. Coordinar con INDOTEL.
5. Coordinar con el Ministerio Público.
6. Coordinar con proveedores tecnológicos.
7. Consolidar información.
8. Identificar riesgos nacionales.
9. Proponer medidas correctivas.
10. Preparar informes periódicos.
11. Coordinar auditorías.
12. Supervisar los procesos de certificación.

RD Propone RD Propone

12. Centro Nacional de Monitoreo

El Centro Nacional de Monitoreo, establecido en capítulos anteriores, deberá funcionar como componente técnico-operativo de la arquitectura nacional. No deberá convertirse en una autoridad paralela. Su función será:

- Recibir información;
- Analizar eventos;
- Generar alertas;
- Apoyar investigaciones;
- Identificar patrones;
- Informar a las autoridades competentes.

13. Centro de Control de cada establecimiento

Cada establecimiento deberá contar con un responsable de seguridad tecnológica. Este funcionario será responsable de:

- Verificar disponibilidad
- Supervisar operadores
- Recibir incidentes
- Activar protocolos
- Garantizar registros
- Reportar fallas
- Coordinar mantenimiento

Deberá existir una cadena clara de mando.

14. Matriz de responsabilidades

Cada proceso deberá contar con una matriz que identifique:

Función	Responsable principal	Apoyo	Supervisión
Seguridad del establecimiento	DGSPC	Personal penitenciario	Ministerio de Justicia
Tecnología	Unidad técnica/DGSPC	Proveedores	Ministerio de Justicia
Telecomunicaciones	INDOTEL	Unidad técnica	Autoridad competente

RD Propone RD Propone

Investigación penal	Ministerio Público	Policía y DGSPC	Autoridad judicial cuando corresponda
Evidencia	Autoridad actuante	Personal técnico	Ministerio Público/Poder Judicial según fase
Contratación	Institución contratante	Unidad técnica	Órganos de control
Auditoría	Órgano competente	Auditores especializados	Autoridad correspondiente
Evaluación nacional	Ministerio de Justicia	Unidad de Coordinación	Instancias de control

La matriz deberá actualizarse cuando cambie la legislación.

15. Protocolo nacional de incidentes

Deberá existir un protocolo único para los incidentes relacionados con:

- Dispositivos;
- Comunicaciones;
- Manipulación tecnológica;
- Corrupción;
- Acceso no autorizado;
- Sabotaje;
- Pérdida de evidencia.

El protocolo deberá establecer:

Quién detecta / *Quién confirma* / *Quién interviene* / *Quién documenta* / *Quién investiga* / *Quién informa*

16. Clasificación de incidentes

Los incidentes deberán clasificarse como:

Nivel I - Incidente técnico Falla sin indicios de conducta ilícita.

Nivel II - Incidente de seguridad Violación de un control o detección de actividad sospechosa.

Nivel III - Incidente disciplinario Conducta atribuible a una persona sujeta al régimen disciplinario.

Nivel IV - Incidente penal Existencia de indicios de un hecho delictivo.

RD Propone RD Propone

Nivel V - Incidente crítico	Evento que pueda comprometer significativamente la seguridad del establecimiento o revelar una estructura organizada.

17. Comunicación inmediata

Los incidentes de niveles superiores deberán activar mecanismos de comunicación predeterminados. La comunicación deberá ser:

- Rápida
- Documentada
- Trazable
- Proporcional
- Dirigida exclusivamente a las autoridades competentes

Deberá evitarse la circulación informal de información sensible.

18. Protección de la evidencia

Toda institución que intervenga en un incidente deberá proteger la evidencia hasta que sea entregada a la autoridad competente. Ningún funcionario deberá:

- Borrar información
- Modificar registros
- Manipular dispositivos innecesariamente
- Eliminar grabaciones
- Alterar bitácoras

Toda intervención deberá quedar documentada.

19. Coordinación con proveedores

Los contratos deberán establecer mecanismos de notificación cuando ocurra:

- Falla crítica
- Ataque informático
- Pérdida de información
- Interrupción de servicio
- Vulnerabilidad de seguridad
- Manipulación del sistema

RD Propone RD Propone

El proveedor no deberá poder decidir unilateralmente si un incidente es suficientemente grave para ser informado. Los criterios deberán estar definidos contractualmente.

20. Consejo técnico interinstitucional

Se propone establecer un consejo técnico permanente integrado por representantes de:

- Ministerio de Justicia;
- Dirección General de Servicios Penitenciarios y Correccionales
- Ministerio Público
- INDOTEL
- Policía Nacional
- Especialistas tecnológicos
- Especialistas jurídicos
- Expertos en ciberseguridad
- Expertos en infraestructura

El consejo tendrá carácter técnico y de coordinación.

No sustituirá las competencias legales de las instituciones representadas.

21. Reuniones y seguimiento

El consejo deberá reunirse periódicamente.

Deberá revisar:

- Incidentes relevantes
- Indicadores
- Fallas
- Tecnologías
- Nuevas amenazas
- Necesidades presupuestarias
- Modificaciones normativas

Las decisiones deberán quedar documentadas.

22. Protocolo ante incidentes graves

Ante un incidente de alta gravedad deberá activarse una cadena especial:

1. Confirmación.
2. Aseguramiento del área.

RD Propone RD Propone

3. Protección de personas.
4. Preservación de evidencia.
5. Notificación a la autoridad competente.
6. Investigación.
7. Evaluación tecnológica.
8. Identificación de vulnerabilidad.
9. Medida correctiva.
10. Auditoría posterior.

23. Investigación posterior al incidente

Todo incidente grave deberá generar un análisis posterior. El análisis deberá determinar:

- Causa
- Vulnerabilidad
- Responsables
- Fallas de procedimiento
- Fallas tecnológicas
- Fallas humanas
- Respuesta
- Medidas correctivas

El objetivo será evitar la repetición del incidente.

24. Responsabilidad institucional

La existencia de múltiples instituciones participantes no deberá diluir la responsabilidad. Cada incidente deberá permitir determinar:

- Qué institución tenía competencia
- Qué unidad tenía responsabilidad
- Qué funcionario tenía obligación específica
- Qué procedimiento debía ejecutarse
- Qué ocurrió realmente

25. Prohibición de transferencia informal de responsabilidades

Ninguna institución podrá limitarse a señalar que una función "correspondía a otra institución" cuando legalmente tenía una obligación concreta de actuación. La coordinación deberá estar sustentada en protocolos previamente establecidos.

26. Intercambio de información

RD Propone RD Propone

Las instituciones participantes deberán establecer mecanismos legales y seguros para compartir información relevante. El intercambio deberá cumplir:

- Finalidad;
- Necesidad;
- Proporcionalidad;
- Seguridad;
- Trazabilidad;
- Protección de datos.

No deberá existir intercambio indiscriminado de información.

27. Plataforma nacional de coordinación

Se deberá establecer una plataforma digital para gestionar:

- Incidentes
- Alertas
- Investigaciones
- Mantenimiento
- Auitorías
- Vulnerabilidades
- Medidas correctivas

Cada institución deberá acceder solamente a la información necesaria para cumplir sus funciones.

28. Registro de actuaciones

Toda actuación relevante deberá generar un registro. El sistema deberá permitir conocer:

- Quién actuó
- Cuándo
- Qué hizo
- Qué información utilizó
- Qué resultado produjo

La trazabilidad deberá convertirse en una característica permanente del sistema.

29. Coordinación presupuestaria

La planificación tecnológica deberá coordinarse con el proceso presupuestario. No deberá autorizarse una adquisición sin considerar:

RD Propone RD Propone

- Instalación
- Mantenimiento
- Capacitación
- Renovación
- Soporte
- Continuidad

El costo total deberá estar identificado antes de contratar.

30. Coordinación legislativa

Cuando durante la implementación se identifique un vacío jurídico, el Ministerio de Justicia deberá coordinar la preparación de la reforma correspondiente con las instituciones competentes.

La legislación deberá evolucionar junto con la tecnología.

31. Cooperación internacional

El Estado podrá establecer acuerdos de cooperación técnica con:

- Organismos internacionales
- Universidades
- Centros de investigación
- Instituciones penitenciarias extranjeras
- Organismos especializados en ciberseguridad
- Entidades de telecomunicaciones

La cooperación deberá orientarse principalmente a:

- Capacitación
- Evaluación
- Transferencia de conocimiento
- Investigación
- Estándares
- Buenas prácticas

32. Participación académica

Las universidades nacionales podrán participar en:

- Evaluación tecnológica
- Análisis estadístico

RD Propone RD Propone

- Investigación
- Desarrollo de indicadores
- Formación de especialistas
- Evaluación de impacto

Esto permitirá desarrollar capacidades nacionales y reducir dependencia externa.

33. Revisión anual de la gobernanza

La estructura institucional deberá evaluarse anualmente. La evaluación deberá determinar:

- Si existen duplicidades
- Si existen vacíos
- Si las instituciones responden oportunamente
- Si los protocolos funcionan
- Si los datos llegan a quien los necesita
- Si existen obstáculos legales

34. Principio de una sola cadena de responsabilidad

La arquitectura institucional deberá poder resumirse de la siguiente manera:

MINISTERIO DE JUSTICIA
Rectoría y coordinación de política pública.
DGSPC
Administración y operación penitenciaria.
CENTROS PENITENCIARIOS
Ejecución diaria de los controles.
CENTRO NACIONAL DE MONITOREO
Análisis, alertas e inteligencia penitenciaria.
INDOTEL
Regulación y coordinación especializada en telecomunicaciones.
MINISTERIO PÚBLICO
Investigación y persecución penal cuando corresponda.
PODER JUDICIAL
Control jurisdiccional y decisiones judiciales dentro de sus competencias.
Los órganos de control y auditoría actuarán transversalmente dentro de sus atribuciones.

35. Resultado esperado

RD Propone RD Propone

Al finalizar la implementación deberá ser posible identificar, ante cualquier incidente relevante:

Qué ocurrió, Dónde ocurrió, Cuándo ocurrió, Quién lo detectó, Quién debía responder, Quién respondió, Qué evidencia existe, Quién investiga, Qué vulnerabilidad permitió el incidente y Qué medida se adoptó para evitar su repetición.

Cuando el Estado pueda responder estas preguntas de manera sistemática, la seguridad penitenciaria dejará de depender exclusivamente de la experiencia individual de determinados funcionarios y comenzará a funcionar como una verdadera política pública institucionalizada.

CAPÍTULO XVI
PREVENCIÓN, COMUNICACIÓN LEGÍTIMA, REINSERCIÓN Y REDUCCIÓN DE INCENTIVOS PARA EL USO CLANDESTINO DE DISPOSITIVOS

1. Objeto del capítulo

El presente capítulo establece las medidas destinadas a complementar las acciones de control tecnológico, físico, operativo y disciplinario previstas en los capítulos anteriores mediante la creación de mecanismos institucionales que permitan atender, de manera legítima, segura y supervisada, las necesidades de comunicación de las personas privadas de libertad.

La seguridad penitenciaria no debe descansar exclusivamente en la prohibición, detección y sanción del uso clandestino de dispositivos electrónicos. Debe incorporar igualmente mecanismos institucionales que reduzcan las razones prácticas por las cuales una persona privada de libertad pudiera procurar o utilizar canales clandestinos de comunicación.

El objetivo es establecer un modelo basado en dos líneas simultáneas:

1. Reducir progresivamente la posibilidad de utilizar dispositivos y comunicaciones clandestinas para coordinar actividades ilícitas.
2. Garantizar canales institucionales suficientes, seguros y verificables para las comunicaciones legítimas.

La combinación de ambas líneas deberá ser evaluada mediante indicadores objetivos, de manera que las autoridades puedan determinar cuáles medidas producen resultados efectivos y cuáles requieren modificación.

RD Propone RD Propone

2. Principio de comunicación legítima como componente de seguridad

La comunicación legítima de las personas privadas de libertad con sus familiares, abogados, representantes consulares y otras personas autorizadas deberá ser considerada un componente de la gestión penitenciaria y no únicamente como un servicio accesorio.

El sistema deberá procurar que las comunicaciones legítimas sean:

- Accesibles;
- Programadas;
- Verificables;
- Seguras;
- Técnicamente controladas;
- Razonablemente disponibles;
- Compatibles con las condiciones particulares de cada establecimiento;
- Respetuosas de los derechos reconocidos por el ordenamiento jurídico.

El propósito no será crear comunicaciones irrestrictas, sino sustituir progresivamente la necesidad de recurrir a mecanismos clandestinos por canales institucionales confiables.

3. Sistema institucional de telefonía penitenciaria

El Estado deberá establecer un sistema de telefonía institucional destinado exclusivamente a comunicaciones autorizadas.

El sistema podrá utilizar terminales fijas, cabinas controladas u otras soluciones tecnológicas que permitan:

- Identificar al usuario
- Registrar fecha y hora de utilización
- Identificar el terminal utilizado
- Administrar listas de contactos autorizados
- Establecer límites razonables de duración
- Generar registros técnicos
- Detectar patrones anómalos
- Impedir modificaciones no autorizadas
- Permitir auditorías
- Garantizar continuidad operacional

RD Propone RD Propone

El sistema deberá diseñarse de manera que la institución pueda determinar quién utilizó el servicio, cuándo, desde qué terminal y bajo qué autorización, sin convertir esa trazabilidad en una vigilancia indiscriminada.

Los registros deberán estar sometidos a las reglas aplicables de protección de datos, seguridad de la información y acceso legítimo.

4. Videocomunicación institucional

De manera progresiva, los establecimientos penitenciarios deberán disponer de espacios destinados a videocomunicaciones supervisadas técnicamente. Estos espacios podrán ser utilizados para:

- Comunicación familiar;
- Comunicación con hijos y familiares que se encuentren lejos;
- Comunicaciones con abogados cuando jurídicamente proceda;
- Comunicación consular;
- Determinados procedimientos administrativos;
- Programas educativos;
- Actividades de reinserción.

Las videocomunicaciones deberán contar con mecanismos de reserva, identificación y registro de utilización. La supervisión deberá diferenciar entre comunicaciones sujetas a control penitenciario ordinario y aquellas comunicaciones que, por su naturaleza jurídica, requieran garantías especiales de confidencialidad.

5. Comunicaciones con abogados y asistencia jurídica

El sistema deberá garantizar mecanismos específicos para facilitar la comunicación entre las personas privadas de libertad y sus abogados.

Estos mecanismos deberán evitar que las medidas generales de seguridad tecnológica terminen obstaculizando indebidamente el ejercicio del derecho de defensa.

Cuando una comunicación requiera confidencialidad jurídica, los sistemas tecnológicos deberán permitir su realización bajo las garantías correspondientes.

La seguridad penitenciaria no deberá utilizarse como justificación automática para eliminar las garantías propias de la defensa.

Por el contrario, el sistema deberá procurar una diferenciación técnica y administrativa entre:

RD Propone RD Propone

- Comunicación familiar
- Comunicación social autorizada
- Comunicación consular
- Comunicación jurídica
- Comunicación administrativa
- Comunicación educativa

Esta clasificación permitirá aplicar controles diferenciados y evitar soluciones generales que produzcan restricciones innecesarias.

6. Comunicaciones consulares

Los ciudadanos extranjeros privados de libertad deberán disponer de mecanismos institucionales para comunicarse con las representaciones consulares correspondientes, de acuerdo con la legislación nacional y las obligaciones internacionales aplicables.

La administración penitenciaria deberá establecer procedimientos claros para:

- Solicitar la comunicación
- Verificar la representación
- Programar la comunicación
- Registrar la utilización del servicio
- Documentar incidencias
- Garantizar las condiciones especiales que correspondan

Este mecanismo deberá integrarse al sistema general de comunicaciones legítimas.

7. Registro de contactos autorizados

Cada persona privada de libertad deberá disponer de un mecanismo administrativo para solicitar la incorporación de contactos autorizados. El sistema deberá establecer:

- Procedimiento de solicitud
- Verificación de identidad
- Criterios objetivos de autorización
- Procedimiento de actualización
- Eliminación de contactos cuando corresponda
- Mecanismos de revisión
- Registro de decisiones
- Controles contra la suplantación de identidad

RD Propone RD Propone

Cuando existan razones legales o de seguridad que justifiquen una restricción, ésta deberá quedar documentada y sometida a los mecanismos de revisión correspondientes.

El objetivo es evitar que la administración de contactos dependa de procedimientos informales o de decisiones no documentadas.

8. Horarios y disponibilidad razonable

La disponibilidad de los servicios de comunicación deberá organizarse mediante horarios previamente establecidos y comunicados. La planificación deberá considerar:

- Población del establecimiento
- Cantidad de terminales disponibles
- Necesidades familiares
- Población trabajadora o estudiantil
- Personas con necesidades especiales
- Distancia geográfica de familiares
- Capacidad operativa del establecimiento

La administración deberá evitar que la insuficiencia de terminales o de horarios convierta el sistema legítimo en un mecanismo meramente nominal.

Cuando la demanda exceda la capacidad disponible, deberán establecerse mecanismos transparentes de asignación.

9. Acceso mínimo garantizado

El sistema deberá estudiar la creación de un nivel mínimo de comunicación institucional para aquellas personas que carezcan de recursos económicos suficientes.

La finalidad será impedir que la capacidad económica determine quién puede mantener contacto regular con su núcleo familiar. Las modalidades podrán incluir:

- Minutos institucionales
- Comunicaciones subvencionadas
- Horarios gratuitos
- Programas sociales
- Mecanismos de colaboración con organizaciones autorizadas

Cualquier programa de este tipo deberá contar con controles presupuestarios y mecanismos de auditoría.

10. Alfabetización digital

RD Propone RD Propone

La transformación tecnológica del sistema penitenciario deberá acompañarse de programas básicos de alfabetización digital. Estos programas podrán incluir:

- Utilización de plataformas institucionales
- Videocomunicación
- Trámites digitales autorizados
- Educación digital
- Seguridad informática básica
- Identificación de fraudes
- Uso responsable de tecnologías
- Preparación para la vida posterior al cumplimiento de la pena.

El objetivo no será simplemente enseñar a utilizar dispositivos, sino desarrollar competencias digitales compatibles con la reinserción social.

11. Servicios digitales controlados

La administración podrá desarrollar plataformas digitales de acceso restringido destinadas a determinados servicios. Entre ellos podrán encontrarse:

- Educación
- Biblioteca digital
- Cursos
- Capacitación laboral
- Orientación jurídica
- Información institucional
- Solicitudes administrativas
- Programas de reinserción
- Comunicación institucional

Estos servicios deberán funcionar dentro de redes controladas y separadas de Internet abierta cuando ello resulte técnicamente necesario.

No deberá confundirse el acceso digital institucional con el acceso irrestricto a redes sociales, aplicaciones de mensajería o servicios externos.

12. Comunicación familiar como instrumento de reinserción

El sistema deberá reconocer la importancia de preservar, cuando sea posible y jurídicamente procedente, los vínculos familiares durante el cumplimiento de la pena.

RD Propone RD Propone

Por ello deberán desarrollarse mecanismos que faciliten:

- Comunicación con padres
- Comunicación con hijos
- Comunicación con cónyuges o parejas
- Comunicación con hermanos
- Comunicación con otros familiares autorizados

La política deberá prestar especial atención a los menores de edad que mantengan vínculos familiares con personas privadas de libertad.

Podrán desarrollarse horarios especiales y mecanismos de videocomunicación para aquellos casos en los que la distancia geográfica dificulte las visitas presenciales.

La finalidad será complementar, no sustituir automáticamente, las visitas físicas.

13. Educación, trabajo y actividades de reinserción

El sistema de seguridad deberá coordinarse con los programas educativos, laborales y de reinserción.

La persona privada de libertad deberá contar, dentro de las posibilidades institucionales, con oportunidades estructuradas para:

- Educación formal
- Formación técnica
- Capacitación laboral
- Actividades productivas
- Programas de comportamiento
- Preparación para la libertad
- Orientación familiar
- Desarrollo de habilidades

Desde la perspectiva de esta política, estas actividades tienen además una función de seguridad: mantener una estructura institucional organizada reduce espacios de inactividad y facilita la identificación de comportamientos que requieran atención.

Esta hipótesis deberá ser evaluada mediante indicadores y no asumida automáticamente como resultado.

14. Canal institucional de solicitudes y reclamaciones

RD Propone RD Propone

Deberá establecerse un canal seguro mediante el cual las personas privadas de libertad puedan presentar:

- Solicitudes
- Reclamaciones
- Denuncias
- Peticiones administrativas
- Reportes sobre problemas de servicios
- Comunicaciones relacionadas con amenazas o situaciones de riesgo

El sistema podrá combinar:

- Terminales físicas
- Formularios
- Sistemas digitales
- Buzones seguros
- Mecanismos de atención presencial

La existencia de canales institucionales accesibles puede permitir que determinados problemas sean detectados antes de transformarse en conflictos mayores.

Las denuncias sensibles deberán contar con mecanismos especiales de confidencialidad y protección frente a represalias, conforme a la legislación aplicable.

15. Protección de víctimas y personas en situación de riesgo

El sistema de comunicaciones legítimas deberá incorporar mecanismos destinados a impedir que una persona privada de libertad utilice los servicios institucionales para contactar indebidamente a:

- Víctimas
- Testigos
- Denunciantes
- Personas protegidas
- Personas respecto de las cuales exista una prohibición judicial
- Otras personas cuya protección haya sido ordenada por autoridad competente

Las restricciones deberán estar fundamentadas en decisiones legales o administrativas debidamente documentadas.

La administración penitenciaria deberá evitar tanto la ausencia de controles como las restricciones arbitrarias.

RD Propone RD Propone

16. Cumplimiento institucional y beneficios dentro del marco legal

El sistema podrá estudiar mecanismos de reconocimiento institucional del cumplimiento de las reglas de seguridad y convivencia, siempre dentro del marco legal vigente.

Estos mecanismos nunca deberán convertirse en premios discrecionales ni afectar derechos que correspondan legalmente. Podrán utilizarse, cuando la normativa lo permita, como elementos de evaluación para programas de:

- Reinserción
- Capacitación
- Participación educativa
- Preparación para la libertad
- Actividades laborales
- Programas de convivencia

El principio será sencillo:

El cumplimiento de las reglas debe tener consecuencias institucionalmente previsibles, pero nunca arbitrarias.

17. Programas de comportamiento y reinserción

Los programas de reinserción deberán incorporar, cuando corresponda, componentes relacionados con:

- Resolución de conflictos
- Responsabilidad personal
- Manejo de impulsos
- Habilidades laborales
- Educación financiera
- Alfabetización digital
- Convivencia
- Responsabilidad familiar
- Preparación para la libertad

Estos programas deberán ser evaluables.

La administración deberá identificar cuáles programas presentan mejores resultados y cuáles requieren modificaciones. No deberá mantenerse indefinidamente un programa

RD Propone RD Propone

simplemente porque exista en el presupuesto; deberá demostrarse su utilidad mediante indicadores.

18. Preparación para la salida

El control penitenciario no termina con la salida de la persona del establecimiento. Deberán fortalecerse programas de transición que incluyan, según corresponda:

- Documentación personal
- Orientación laboral
- Capacitación
- Vinculación con servicios públicos
- Orientación familiar
- Información sobre obligaciones legales
- Educación financiera
- Prevención de reincidencia
- Orientación digital

Cuando resulte jurídicamente procedente, podrán establecerse mecanismos de coordinación con instituciones externas para facilitar la continuidad de determinados servicios.

19. Capacitación del personal

El personal penitenciario deberá recibir formación específica sobre:

- Utilización de los sistemas de comunicación institucional;
- Derechos de las personas privadas de libertad;
- Protección de datos
- Seguridad informática
- Detección de usos indebidos
- Protocolos de incidentes
- Preservación de evidencia
- Prevención de corrupción
- Manejo de situaciones de conflicto

La capacitación deberá actualizarse cuando se incorporen nuevas tecnologías. Ningún sistema tecnológico deberá considerarse plenamente implementado mientras los funcionarios encargados de utilizarlo no hayan recibido la formación correspondiente.

20. Indicadores de utilización de las comunicaciones legítimas

RD Propone RD Propone

El Sistema Nacional de Indicadores deberá incorporar información sobre el funcionamiento de las comunicaciones institucionales. Entre otros indicadores podrán medirse:

- Número de comunicaciones realizadas
- Porcentaje de solicitudes atendidas
- Tiempo promedio de espera
- Disponibilidad de terminales
- Fallas técnicas
- Duración promedio
- Cantidad de videollamadas
- Comunicaciones jurídicas
- Comunicaciones consulares
- Comunicaciones familiares
- Utilización por establecimiento
- Interrupciones del servicio
- Reclamaciones
- Satisfacción de usuarios mediante mecanismos apropiados

Estos datos permitirán determinar si el sistema realmente constituye una alternativa funcional a los canales clandestinos.

21. Indicadores sobre reducción de comunicaciones clandestinas

La política deberá establecer indicadores específicos para evaluar la hipótesis de que el fortalecimiento de canales legítimos puede contribuir a reducir determinados incentivos para el uso clandestino. Podrán analizarse, entre otros:

- Dispositivos clandestinos incautados;
- Intentos de introducción;
- Eventos de detección;
- Frecuencia de uso no autorizado;
- Reincidencia;
- Participación de personal interno;
- Intentos de manipulación tecnológica;
- Patrones por establecimiento;
- Relación entre disponibilidad de comunicación legítima y eventos clandestinos.

RD Propone RD Propone

La evaluación deberá controlar otros factores relevantes para evitar atribuir automáticamente una disminución o aumento a una sola medida.

22. Programa piloto

Antes de aplicar el modelo nacional, el Ministerio de Justicia y las instituciones competentes podrán seleccionar establecimientos representativos para desarrollar programas piloto. Los pilotos deberán permitir comparar:

- Establecimientos con diferentes niveles de riesgo;
- Diferentes niveles de infraestructura;
- Diferentes densidades poblacionales;
- Diferentes capacidades tecnológicas.

Cada piloto deberá establecer una línea base previa y una evaluación posterior. Deberá documentarse:

1. Costo
2. Disponibilidad
3. Utilización
4. Incidentes
5. Fallas
6. Percepción de usuarios
7. Comportamiento del sistema
8. Efectos no previstos

Los resultados deberán determinar qué componentes pueden escalarse y cuáles requieren modificación.

23. Protección de datos y límites de vigilancia

Toda recolección, conservación, consulta o intercambio de información deberá responder a una finalidad legítima y encontrarse sometida a los controles establecidos por la legislación aplicable. Deberán establecerse:

- Perfiles de acceso;
- Registros de consulta;
- Autenticación
- Conservación limitada
- Mecanismos de eliminación
- Auditoría

RD Propone RD Propone

- Protección contra accesos no autorizados
- Protocolos de incidentes de seguridad

La información obtenida mediante estos sistemas no deberá utilizarse para fines distintos de aquellos legalmente autorizados.

24. Principio de sustitución funcional

La política nacional deberá adoptar como criterio de diseño el siguiente principio:

No basta con retirar un dispositivo clandestino; es necesario sustituir, mediante mecanismos legítimos, las funciones legítimas que ese dispositivo estaba permitiendo realizar.

Esto no significa reconocer ningún derecho a poseer teléfonos personales dentro de los establecimientos cuando la normativa los prohíba. Significa reconocer que la política de seguridad será más completa cuando combine:

Restricción / Detección / Investigación / Sanción / Comunicación legítima / Reinserción

De esta manera, la política no dependerá exclusivamente de una carrera tecnológica entre quienes intentan introducir dispositivos clandestinos y las autoridades que intentan detectarlos.

25. Integración con el Sistema Nacional de Seguridad Penitenciaria

Las medidas establecidas en este capítulo deberán integrarse con:

- El sistema de control de acceso;
- Los sistemas de detección
- El Centro Nacional de Monitoreo
- Los mecanismos de inteligencia
- Los protocolos de investigación
- Los sistemas de videovigilancia
- Los programas de reinserción
- El sistema de indicadores
- Las auditorías
- El régimen disciplinario

La comunicación legítima no deberá operar como un sistema aislado. Deberá formar parte de una arquitectura institucional única.

26. Evaluación periódica

RD Propone RD Propone

Cada establecimiento deberá presentar periódicamente información sobre:

- Funcionamiento de las comunicaciones legítimas;
- Demanda
- Capacidad disponible
- Fallas
- Incidentes
- Intentos de utilización indebida
- Costos
- Mantenimiento
- Resultados

El Ministerio de Justicia deberá consolidar esta información y utilizarla para ajustar la política nacional. Los establecimientos con niveles elevados de incidentes deberán ser sometidos a análisis específicos para determinar si existen deficiencias de infraestructura, personal, tecnología, procedimientos, corrupción, sobrepoblación u otros factores.

27. Principio final del capítulo

La seguridad penitenciaria moderna no debe plantearse exclusivamente como una lucha entre la administración y quienes intentan vulnerar sus controles. Debe construirse un sistema en el que la comunicación legítima sea fácil de utilizar, la comunicación clandestina sea difícil de introducir, el uso clandestino sea detectable, la manipulación sea investigable, la complicidad sea sancionable, la evidencia sea preservable, y la reinserción sea medible.

El objetivo final no es simplemente impedir que exista un teléfono clandestino dentro de una prisión.

El objetivo es reducir la capacidad de los establecimientos penitenciarios para convertirse en plataformas de coordinación criminal, mientras se mantiene un sistema compatible con la dignidad humana, el debido proceso, el derecho de defensa, la protección de las víctimas y los objetivos legítimos de reinserción social.

28. Resultado esperado

La aplicación conjunta de este capítulo con las medidas de los capítulos anteriores deberá permitir avanzar hacia un modelo en el cual la seguridad penitenciaria no dependa de una sola tecnología ni de una sola institución. El modelo deberá funcionar mediante cinco capas complementarias:

RD Propone RD Propone

1. Prevención: impedir la entrada de dispositivos no autorizados.
2. Detección: identificar oportunamente su presencia o utilización.
3. Respuesta: intervenir de manera rápida, proporcional y documentada.
4. Investigación: determinar cómo ingresó el dispositivo, quién participó y qué actividades fueron coordinadas.
5. Sustitución legítima: ofrecer mecanismos institucionales suficientes para las necesidades legítimas de comunicación, educación, asistencia jurídica y reinserción.
De esta forma, el programa pasa de ser exclusivamente un proyecto de *"control de celulares en las cárceles"* a convertirse en una política integral de *seguridad, inteligencia, comunicación institucional y reinserción penitenciaria.*

CAPÍTULO XVII
MARCO CONSTITUCIONAL, LEGAL Y DE DERECHOS FUNDAMENTALES

1. Objeto

El presente capítulo establece los principios constitucionales y legales que deberán regir el diseño, implementación, operación, supervisión y evaluación del Sistema Nacional de Seguridad Tecnológica Penitenciaria.

Su finalidad es garantizar que las medidas de seguridad propuestas sean compatibles con:

- La Constitución de la República Dominicana
- La legislación penitenciaria vigente
- La legislación procesal penal
- La legislación sobre telecomunicaciones
- La legislación sobre protección de datos personales
- Las normas de la Administración Pública
- Los tratados internacionales aplicables
- La jurisprudencia constitucional
- y las demás disposiciones que resulten aplicables

La existencia de un objetivo legítimo de seguridad no elimina la obligación del Estado de actuar conforme a la Constitución y las leyes.

2. Principio de supremacía constitucional

Toda actuación realizada dentro del Sistema deberá someterse a la Constitución de la República.

RD Propone RD Propone

Ninguna disposición administrativa, protocolo, contrato, manual operativo, especificación técnica o decisión institucional podrá establecer válidamente una restricción de derechos que carezca del fundamento jurídico correspondiente.

Cuando exista conflicto entre una práctica operativa y una norma constitucional o legal, deberá prevalecer el ordenamiento jurídico.

3. Situación jurídica de las personas privadas de libertad

La privación de libertad no elimina la condición de persona titular de derechos fundamentales.

La Ley 113-21 establece como fundamentos del sistema penitenciario la dignidad humana, la rehabilitación y la reinserción social. Por tanto, el sistema deberá distinguir entre:

1. Derechos que resulten necesariamente restringidos por la propia sentencia y la privación de libertad;
2. Derechos que permanezcan plenamente protegidos;
3. Derechos cuya limitación pueda resultar jurídicamente admisible por razones de seguridad, disciplina, salubridad o reinserción.

Toda restricción deberá contar con fundamento jurídico y guardar relación con la finalidad perseguida.

4. Principio de legalidad

Las medidas de seguridad que afecten derechos fundamentales deberán encontrarse sustentadas en una norma con rango suficiente.

No podrá utilizarse una simple circular, protocolo interno o decisión administrativa para crear restricciones que la Constitución o la ley hayan reservado al legislador. Este principio resulta especialmente importante respecto de:

- Interceptación de comunicaciones
- Acceso a contenido de comunicaciones
- Tratamiento de datos personales
- Utilización de información obtenida mediante sistemas tecnológicos
- Restricciones de comunicación
- Registros
- Vigilancia

RD Propone RD Propone

- Medidas disciplinarias
- Utilización de evidencia tecnológica

5. Derecho a la intimidad y secreto de las comunicaciones

La jurisprudencia del Tribunal Constitucional ha establecido que la protección comprende las comunicaciones independientemente del medio utilizado y que su intervención válida requiere las garantías previstas constitucional y legalmente.

De igual manera, una sentencia reciente del Tribunal Constitucional, TC/1278/25, reiteró que la interceptación, captación o grabación de comunicaciones requiere habilitación legal y, en los casos correspondientes, autorización judicial; además, señaló que una actuación administrativa no puede crear por sí sola una facultad de interceptación no prevista legalmente.

En consecuencia, el presente proyecto deberá diferenciar claramente entre:

A. Detección técnica de la existencia de un dispositivo.
B. Localización técnica de un dispositivo.
C. Identificación técnica de determinados parámetros del dispositivo, cuando legalmente proceda.
D. Interceptación o captación del contenido de comunicaciones.
Estas categorías no podrán ser tratadas como si fueran jurídicamente equivalentes.

6. Prohibición de vigilancia indiscriminada

El Sistema no deberá diseñarse para convertir los establecimientos penitenciarios en espacios de vigilancia tecnológica ilimitada. La utilización de herramientas de seguridad deberá responder a una finalidad concreta y legítima. Deberán establecerse mecanismos que permitan determinar:

- Qué información se obtiene
- Por qué se obtiene
- Quién puede acceder
- Durante cuánto tiempo se conserva
- Con qué finalidad puede utilizarse
- Quién autoriza el acceso
- Quién supervisa el procedimiento

La mera disponibilidad tecnológica no constituirá autorización jurídica para utilizar una determinada capacidad.

RD Propone RD Propone

7. Detección no equivale a interceptación

Este principio deberá quedar expresamente incorporado al diseño normativo.

Un sistema destinado a detectar la posible presencia de un dispositivo no deberá configurarse automáticamente para captar el contenido de sus comunicaciones. Por ello, las soluciones tecnológicas deberán priorizar, cuando sea suficiente para cumplir la finalidad de seguridad:

- Detección
- Alerta
- Localización
- Identificación técnica
- Análisis de patrones no relacionados con el contenido
- Respuesta operativa

Cuando una investigación requiera acceder al contenido de comunicaciones, deberá aplicarse el procedimiento legal correspondiente.

8. Proporcionalidad

Toda medida restrictiva deberá responder a una finalidad legítima y mantener una relación razonable entre:

Riesgo identificado / Medida aplicada / Intensidad de la restricción / Resultado esperado

No deberá utilizarse una medida de máxima intensidad cuando una medida menos invasiva sea suficiente para alcanzar el mismo objetivo de seguridad.

Este principio deberá incorporarse tanto a la legislación como a los reglamentos y protocolos técnicos.

9. Necesidad

Antes de incorporar una nueva tecnología deberá determinarse:

1. Cuál problema pretende resolver
2. Cuál es el riesgo
3. Qué alternativas existen
4. Cuál es la alternativa menos restrictiva
5. Qué evidencia técnica justifica la solución
6. Cuál será su costo

RD Propone RD Propone

7. Cuáles serán sus efectos sobre los derechos fundamentales

La adquisición deberá producirse después de esta evaluación y no antes.

10. Debido proceso administrativo y disciplinario

Las medidas disciplinarias derivadas del hallazgo o utilización de dispositivos no autorizados deberán respetar las garantías correspondientes.

La existencia de una alerta tecnológica no deberá considerarse automáticamente prueba definitiva de responsabilidad individual. Deberán distinguirse:

- Alerta
- Hallazgo
- Evidencia
- Identificación del responsable
- Investigación
- Decisión disciplinaria
- Eventual investigación penal

Esta separación es esencial para evitar que un sistema automatizado produzca sanciones sin intervención humana y sin las garantías correspondientes. La jurisprudencia constitucional reconoce que las garantías del debido proceso alcanzan también las actuaciones administrativas.

11. Presunción y valoración de evidencia tecnológica

Los datos producidos por sistemas tecnológicos deberán ser tratados como elementos de información o evidencia sujetos a valoración conforme al procedimiento correspondiente. Una alerta podrá justificar:

- Inspección
- Verificación
- Preservación de evidencia
- Investigación

Pero no deberá sustituir automáticamente la investigación necesaria para establecer responsabilidad. Los sistemas deberán mantener:

- Fecha y hora
- Identificación del sistema
- Operador

RD Propone RD Propone

- Configuración
- Registro de eventos
- Modificaciones
- Mantenimiento
- Cadena de custodia cuando corresponda

12. Protección de datos personales

El Sistema deberá cumplir con las normas aplicables sobre protección de datos personales. Esto será especialmente relevante respecto de:

- Datos de personas privadas de libertad
- Familiares
- Abogados
- Visitantes
- Funcionarios
- Proveedores
- Registros de llamadas
- Registros de acceso
- Imágenes
- Información biométrica
- Identificadores tecnológicos
- Información utilizada para inteligencia

El tratamiento deberá responder a principios de legalidad, finalidad, seguridad, calidad y demás garantías aplicables. El Tribunal Constitucional continúa desarrollando jurisprudencia sobre intimidad, autodeterminación informativa y hábeas data; su cuadernillo jurisprudencial publicado en 2026 incluye expresamente aplicaciones de estos derechos al ámbito penitenciario.

13. Información penitenciaria confidencial

La información almacenada en los sistemas penitenciarios deberá contar con controles específicos de acceso y utilización. La Ley 80-25 modificó disposiciones de la Ley 113-21 relativas al Sistema Penitenciario y Correccional, incluyendo reglas sobre información penitenciaria y coordinación institucional.

Por ello, el desarrollo reglamentario del presente programa deberá utilizar la versión vigente de la normativa y no reproducir mecánicamente disposiciones anteriores a la reforma institucional de 2025.

RD Propone RD Propone

14. Nueva arquitectura institucional

Este proyecto deberá ser compatible con la reorganización producida por la Ley 80-25. La referida ley creó el Ministerio de Justicia y modificó disposiciones de la Ley 113-21, incluyendo la estructura institucional vinculada al sistema penitenciario.

La DGSPC permanece como organismo especializado del sistema penitenciario y se encuentra adscrita al Ministerio de Justicia, conforme a las modificaciones introducidas por la Ley 80-25. Por tanto, las responsabilidades propuestas en este proyecto deberán ser asignadas respetando esa arquitectura.

15. Separación entre administración penitenciaria e investigación penal

El Sistema deberá mantener una separación funcional entre *administración penitenciaria y investigación penal.* La administración penitenciaria deberá detectar, prevenir, preservar y comunicar incidentes conforme a sus competencias.

El Ministerio Público deberá ejercer sus funciones investigativas dentro del marco legal correspondiente. Cuando un incidente tecnológico pueda constituir delito, deberá activarse el mecanismo institucional correspondiente para la investigación penal.

Esta separación evita que una herramienta administrativa termine convirtiéndose informalmente en una herramienta de investigación penal sin las garantías necesarias.

16. Coordinación con el Ministerio Público

La Ley 80-25 modificó las reglas de coordinación entre el Ministerio de Justicia y el Ministerio Público respecto del acceso a personas privadas de libertad para investigaciones. Por tanto, el sistema deberá establecer:

- Mecanismo de notificación
- Procedimiento para preservación de evidencia
- Solicitud de información
- Acceso a registros
- Coordinación de investigaciones
- Protección de información sensible
- Responsables institucionales
- Tiempos de respuesta

17. Coordinación con INDOTEL

RD Propone RD Propone

Las medidas relacionadas con redes de telecomunicaciones deberán respetar el marco regulatorio del sector.

La Ley General de Telecomunicaciones núm. 153-98 constituye el marco legal general del sector y establece las competencias regulatorias correspondientes.

Por tanto, cualquier solución tecnológica que pueda afectar redes públicas, espectro, servicios de telecomunicaciones o infraestructura de operadores deberá ser evaluada y coordinada con la autoridad competente.

El proyecto deberá evitar establecer en la ley una tecnología específica cuando la evolución tecnológica pueda volverla obsoleta.

18. Neutralidad tecnológica

La legislación deberá definir qué debe lograrse, y no necesariamente qué marca, aparato o tecnología debe comprarse. Por ejemplo, la ley podrá exigir:

"El establecimiento deberá contar con capacidad permanente para detectar y gestionar comunicaciones no autorizadas." Pero no deberá obligar necesariamente a utilizar una determinada marca, modelo o tecnología.

Esto permitirá actualizar los sistemas sin tener que modificar la ley cada vez que aparezca una tecnología nueva.

19. Prohibición de mecanismos tecnológicos lesivos

Queda excluida del modelo cualquier solución destinada deliberadamente a provocar daños físicos, eléctricos o electrónicos a dispositivos mediante métodos que puedan generar riesgos para personas, instalaciones o infraestructura.

La infraestructura eléctrica penitenciaria deberá utilizarse para:

- Seguridad
- Continuidad
- Monitoreo
- Detección de anomalías
- Protección de equipos
- Prevención de incendios
- Gestión energética

No deberá utilizarse como mecanismo improvisado para destruir dispositivos.

RD Propone RD Propone

Esta exclusión deberá quedar expresamente establecida en las especificaciones técnicas y procesos de contratación.

20. Inteligencia artificial y decisiones automatizadas

La utilización de inteligencia artificial podrá incorporarse como herramienta auxiliar para:

- Detección de anomalías
- Análisis de patrones
- Clasificación de alertas
- Mantenimiento predictivo
- Análisis de grandes volúmenes de información
- Identificación de comportamientos técnicos inusuales

Sin embargo, una alerta generada por inteligencia artificial no deberá producir automáticamente:

- Sanciones
- Aislamiento
- Restricciones de derechos
- Imputaciones
- Decisiones disciplinarias

Deberá existir intervención humana competente y trazabilidad de la decisión.

21. Derecho de revisión

Las personas afectadas por una decisión administrativa deberán disponer de los mecanismos de revisión que establezca el ordenamiento jurídico. Esto será especialmente importante cuando una decisión se base total o parcialmente en:

- Registros tecnológicos
- Sistemas automatizados
- Identificación biométrica
- Análisis algorítmico
- Informes de inteligencia
- Alertas electrónicas

El sistema deberá permitir corregir errores técnicos o humanos.

22. Contratación pública y seguridad tecnológica

RD Propone RD Propone

La contratación de sistemas de seguridad deberá someterse a la legislación vigente de contrataciones públicas.

No deberá utilizarse la naturaleza penitenciaria de una adquisición como justificación automática para excluirla de los procedimientos ordinarios.

Cuando una contratación pueda quedar comprendida dentro de un régimen especial de seguridad nacional, deberán cumplirse estrictamente las condiciones legales y reglamentarias correspondientes.

La existencia de procedimientos de excepción previstos por la legislación de contrataciones no elimina las obligaciones de control, documentación y responsabilidad pública.

En 2026 existen normas específicas que regulan procedimientos de excepción por razones de seguridad nacional, por lo que cada contratación deberá analizarse individualmente.

23. Transparencia y reserva

El proyecto deberá encontrar un equilibrio entre transparencia pública y protección de información de seguridad.

Deberán publicarse, cuando jurídicamente proceda:

- Objetivos
- Presupuesto
- Indicadores
- Resultados
- Auditorías
- Estadísticas agregadas
- Cumplimiento de metas
- Incidencias generales

Pero podrán mantenerse reservados los detalles cuya divulgación pueda facilitar:

- Evasión de controles
- Vulneración de sistemas
- Identificación de vulnerabilidades
- Explotación de infraestructura
- Comprometer investigaciones
- Poner en riesgo al personal

RD Propone RD Propone

La reserva deberá tener fundamento jurídico y no utilizarse para ocultar irregularidades.

24. Control externo

El sistema deberá estar sujeto a controles externos compatibles con las competencias de:

- Congreso Nacional
- Cámara de Cuentas
- Contraloría General de la República
- Organos jurisdiccionales
- Ministerio Público
- Organos de protección de derechos
- Autoridades regulatorias
- Demás instituciones competentes

La finalidad será evitar que el sistema de seguridad se convierta en un espacio institucional sin controles.

25. Revisión de constitucionalidad de las medidas

Antes de la implementación nacional de cualquier componente que implique una afectación relevante de derechos fundamentales, deberá realizarse una evaluación jurídica previa.

Esta evaluación deberá determinar:

1. Fundamento legal
2. Finalidad
3. Autoridad competente
4. Derecho afectado
5. Intensidad de la afectación
6. Necesidad
7. Proporcionalidad
8. Procedimiento
9. Mecanismos de revisión
10. Tratamiento de datos
11. Conservación de información
12. Responsabilidad institucional

RD Propone RD Propone

Cuando la evaluación determine que una medida requiere una habilitación legal que actualmente no existe, deberá promoverse primero la correspondiente reforma legislativa.

26. Cláusula de salvaguarda constitucional

Toda disposición reglamentaria, protocolo técnico o procedimiento operativo derivado del presente programa deberá incorporar una cláusula que establezca que su aplicación queda sujeta a:

- La Constitución
- Las leyes
- Los tratados internacionales vigentes
- Las decisiones vinculantes del Tribunal Constitucional
- Las autorizaciones judiciales que correspondan

27. Revisión periódica del marco jurídico

La evolución tecnológica puede producir nuevas situaciones jurídicas, por ello, el Ministerio de Justicia deberá realizar revisiones periódicas del marco normativo aplicable al sistema. Estas revisiones deberán considerar:

- Nuevas tecnologías
- Nuevas modalidades de comunicación
- Jurisprudencia
- Cambios legislativos
- Riesgos de ciberseguridad
- Protección de datos
- Experiencias nacionales
- Experiencias internacionales

Cuando una nueva tecnología produzca una capacidad de vigilancia significativamente superior a las existentes, deberá realizarse una evaluación jurídica específica antes de su despliegue nacional.

28. Principio de mínima intervención

El Estado deberá utilizar la menor intervención compatible con la finalidad legítima de seguridad. En términos prácticos *si detectar es suficiente, no deberá interceptarse; si localizar es suficiente, no deberá accederse al contenido; si una restricción temporal es suficiente, no deberá*

RD Propone RD Propone

imponerse una restricción permanente; si una solución individual es suficiente, no deberá afectarse a toda la población penitenciaria.

Este principio deberá orientar tanto las decisiones operativas como las futuras reformas legislativas.

29. Regla de interpretación

Las disposiciones del presente programa deberán interpretarse de forma que:

- Fortalezcan la seguridad
- Protejan la dignidad humana
- Respeten el debido proceso
- Preserven el derecho de defensa
- Protejan la intimidad
- Garanticen la seguridad de las víctimas
- Permitan investigaciones eficaces
- Eviten la arbitrariedad
- y mantengan la responsabilidad institucional

Cuando exista duda razonable sobre el alcance de una medida que afecte un derecho fundamental, deberá acudirse a la autoridad jurídica competente antes de implementarla.

30. Conclusión jurídica del capítulo

El Sistema Nacional de Seguridad Tecnológica Penitenciaria deberá construirse bajo una premisa fundamental la seguridad del Estado y los derechos fundamentales no deben ser concebidos necesariamente como objetivos incompatibles.

El desafío consiste en diseñar mecanismos que permitan al Estado controlar eficazmente las comunicaciones clandestinas utilizadas para actividades delictivas sin transformar ese control en una autorización general para vigilar, interceptar o recopilar indiscriminadamente las comunicaciones de las personas.

Por ello, el proyecto deberá diferenciar con precisión:

Detectar ≠ Interceptar

Localizar ≠ Escuchar

Registrar un evento ≠ Registrar el contenido de una comunicación

Generar una alerta ≠ Determinar responsabilidad

Investigar ≠ Sancionar automáticamente

RD Propone RD Propone

Seguridad ≠ Vigilancia ilimitada.

El resultado esperado es un sistema que sea simultáneamente eficaz, técnicamente moderno, jurídicamente defendible, auditable y respetuoso de los derechos fundamentales.

Ese equilibrio deberá constituir una condición indispensable para la implementación nacional del programa.

CAPÍTULO XVIII
SISTEMA NACIONAL DE INFORMACIÓN, INTELIGENCIA PENITENCIARIA Y EVIDENCIA DIGITAL

1. Objeto

El presente capítulo establece las bases para la creación de un sistema integrado de información, análisis e inteligencia penitenciaria destinado a identificar, prevenir, investigar y documentar los riesgos relacionados con el uso clandestino de dispositivos electrónicos y comunicaciones no autorizadas dentro de los establecimientos penitenciarios.

El sistema deberá permitir transformar los diferentes registros generados por la administración penitenciaria en información útil para la prevención y la investigación, sin confundir:

Dato / Información / Alerta / Inteligencia / Evidencia / Prueba

Cada una de estas categorías tendrá una finalidad y un régimen de utilización diferente.

2. Principio de finalidad

La información obtenida mediante los sistemas penitenciarios deberá utilizarse exclusivamente para finalidades legítimas y previamente definidas. Entre ellas:

- Prevención de delitos
- Seguridad penitenciaria
- Protección de personas
- Detección de dispositivos no autorizados
- Investigación de incidente
- Identificación de vulnerabilidades
- Prevención de corrupción

RD Propone RD Propone

- Protección de infraestructura
- Evaluación institucional
- Preservación de evidencia

No deberá utilizarse información penitenciaria para finalidades incompatibles con la ley.

3. Arquitectura nacional de información

El sistema deberá integrar, conforme a las competencias legales de cada institución, información procedente de:

- Controles de acceso
- Registros de visitantes
- Registros de proveedores
- Inventarios
- Incautaciones
- Videovigilancia
- Sistemas de detección
- Incidentes
- Mantenimiento tecnológico
- Fallas de infraestructura
- Personal autorizado
- Movimientos internos
- Comunicaciones institucionales
- Auditorías
- Investigaciones
- Sanciones
- Información suministrada por instituciones competentes

La integración deberá realizarse bajo reglas de acceso, seguridad y trazabilidad.

No deberá crearse una base de datos ilimitada que concentre indiscriminadamente toda la información disponible sobre las personas.

4. Clasificación de la información

La información deberá clasificarse, como mínimo, en:

Nivel 1 - Información operacional: Datos necesarios para la operación cotidiana de los establecimientos.

RD Propone RD Propone

Nivel 2 - Información de seguridad: Datos cuya divulgación pueda comprometer controles, infraestructura o procedimientos.

Nivel 3 - Información de inteligencia: Información analizada para identificar riesgos, relaciones, patrones o amenazas.

Nivel 4 - Información investigativa: Información vinculada a investigaciones administrativas o penales.

Nivel 5 - Información reservada o protegida: Información cuyo acceso se encuentre legalmente restringido.

Cada nivel deberá contar con controles específicos de acceso.

5. Registro nacional de incidentes tecnológicos

Deberá establecerse un Registro Nacional de Incidentes de Seguridad Tecnológica Penitenciaria. Este registro deberá documentar, entre otros:

- Fecha
- Hora
- Establecimiento
- Tipo de incidente
- Sistema que generó la alerta
- Naturaleza del evento
- Medidas adoptadas
- Dispositivos incautados
- Personal participante
- Evidencia preservada
- Resultado de la investigación
- Medidas correctivas

El registro deberá permitir identificar reincidencias y patrones.

6. Identificador único de incidentes

Cada incidente deberá recibir un identificador único. Este identificador permitirá relacionar:

- Alerta inicial
- Fotografías
- Videos

RD Propone RD Propone

- Informes
- Actas
- Objetos incautados
- Registros técnicos
- Actuaciones administrativas
- Actuaciones investigativas
- Medidas correctivas

De esta manera, un incidente no quedará distribuido en archivos independientes imposibles de reconstruir.

7. Cadena de custodia

Todo dispositivo electrónico, tarjeta SIM, memoria, computadora, documento u otro elemento que pueda constituir evidencia deberá ser sometido al procedimiento correspondiente de preservación y cadena de custodia. Deberá registrarse:

1. Quién lo encontró
2. Dónde fue encontrado
3. Cuándo fue encontrado
4. Quién lo recibió
5. Cómo fue identificado
6. Cómo fue embalado o protegido
7. Quién lo trasladó
8. Quién lo examinó
9. Qué procedimiento técnico fue realizado
10. Cuándo fue entregado
11. Dónde fue almacenado

La finalidad será garantizar que pueda establecerse posteriormente la integridad del elemento.

8. Evidencia digital

La evidencia digital deberá tratarse con procedimientos especializados. Podrán constituir elementos de interés investigativo, según las circunstancias y autorizaciones correspondientes:

- Dispositivos
- Tarjetas SIM

RD Propone RD Propone

- Registros técnicos
- Archivos
- Imágenes
- Videos
- Metadatos
- Registros de acceso
- Registros de sistemas
- Información de aplicaciones
- Datos obtenidos de infraestructura institucional.

La extracción o análisis de contenido protegido deberá realizarse únicamente conforme al procedimiento legal aplicable.

9. Diferencia entre incautación y extracción de información

La incautación física de un dispositivo no significa automáticamente autorización para acceder a todo su contenido. Esta distinción deberá quedar expresamente incorporada en los protocolos. La actuación deberá diferenciar entre:

a. Localizar un dispositivo
b. Asegurar físicamente el dispositivo
c. Preservar el dispositivo
d. Documentar sus características externas
e. Realizar análisis técnico autorizado
f. Extraer información cuando exista habilitación legal
g. Utilizar la información obtenida en una investigación

La jurisprudencia constitucional dominicana ha reconocido que la extracción de archivos de dispositivos puede requerir autorización judicial y que el ejercicio de facultades investigativas debe respetar las formalidades procesales aplicables.

10. Prohibición de exploración indiscriminada

La administración penitenciaria no deberá realizar exploraciones indiscriminadas del contenido de dispositivos incautados simplemente porque estos se encuentren dentro de un establecimiento penitenciario.

La finalidad de seguridad penitenciaria no elimina las garantías constitucionales aplicables. Cuando una investigación requiera acceder al contenido de un dispositivo, deberá activarse el procedimiento correspondiente ante la autoridad competente.

RD Propone RD Propone

11. Centro Nacional de Inteligencia Penitenciaria

Como componente del sistema creado en capítulos anteriores, deberá establecerse una unidad especializada de análisis de información penitenciaria. Esta unidad podrá:

- Integrar información
- Analizar tendencias
- Identificar patrones
- Elaborar mapas de riesgo
- Detectar anomalías
- Establecer relaciones entre incidentes
- Identificar vulnerabilidades recurrentes
- Producir informes de inteligencia
- Apoyar investigaciones
- Recomendar medidas preventivas

La unidad no sustituirá al Ministerio Público ni a los órganos competentes de investigación criminal.

12. Inteligencia estratégica

La inteligencia estratégica deberá responder preguntas como:

- ¿En qué establecimientos se concentran determinados incidentes?
- ¿Cuáles son las modalidades de introducción más frecuentes?
- ¿Qué controles presentan mayores vulnerabilidades?
- ¿Existen patrones relacionados con determinados horarios?
- ¿Existen patrones relacionados con visitantes o proveedores?
- ¿Se repiten determinados tipos de dispositivos?
- ¿Existen vínculos entre incidentes aparentemente independientes?
- ¿Qué medidas han demostrado reducir determinados riesgos?

La finalidad será anticipar vulnerabilidades y no limitarse a reaccionar después del incidente.

13. Inteligencia operacional

La inteligencia operacional deberá apoyar la gestión cotidiana. Podrá generar:

- Alertas
- Mapas de riesgo

RD Propone RD Propone

- Informes diarios
- Informes semanales
- Análisis de reincidencia
- Identificación de vulnerabilidades
- Recomendaciones de inspección
- Solicitudes de auditoría

Toda alerta deberá diferenciarse claramente de una conclusión de responsabilidad.

14. Análisis de vínculos

El sistema podrá utilizar herramientas de análisis de vínculos para identificar relaciones entre:

- Incidentes
- Dispositivos
- Establecimientos
- Horarios
- Personas
- Visitas
- Proveedores
- Funcionarios
- Eventos

Cuando dicho análisis involucre información personal o datos sensibles, deberá aplicarse el régimen jurídico correspondiente. La herramienta podrá señalar una relación que requiera investigación, pero no deberá convertir automáticamente esa relación estadística en una acusación.

15. Identificación técnica de dispositivos

Cuando legalmente proceda, el sistema podrá registrar características técnicas de dispositivos detectados o incautados. Entre ellas podrían encontrarse:

- Fabricante
- Modelo
- Identificadores técnicos
- Características de red
- Información relacionada con SIM
- Fecha de detección

RD Propone RD Propone

- Ubicación aproximada
- Establecimiento

La utilización de estos identificadores deberá someterse a las reglas aplicables de seguridad y protección de datos.

16. Reincidencia tecnológica

El sistema deberá poder determinar si determinados patrones técnicos se repiten. Por ejemplo:

- Mismo dispositivo
- Mismo identificador técnico
- Mismo patrón de detección
- Misma zona
- Mismo horario
- Misma modalidad de introducción

La reincidencia podrá utilizarse como elemento para priorizar investigaciones y auditorías. No deberá utilizarse automáticamente como prueba de que una persona específica es responsable.

17. Correlación de eventos

Uno de los principales objetivos del Centro Nacional de Monitoreo será permitir la correlación de eventos. Ejemplo conceptual:

Falla de cámara / Entrada de visitante / Anomalía de control / Detección de dispositivo / Desplazamiento interno / Incautación

El sistema deberá permitir reconstruir cronológicamente estos eventos. Esto puede ser mucho más útil que analizar cada registro de manera aislada.

18. Línea de tiempo digital

Cada incidente relevante deberá poder reconstruirse mediante una línea de tiempo. La línea podrá incluir:

- Evento inicial
- Primera alerta
- Intervención del personal
- Ubicación
- Movimientos

RD Propone RD Propone

- Incautación
- Traslado
- Preservación de evidencia
- Notificación
- Investigación
- Resultado

La reconstrucción cronológica deberá formar parte de los informes de incidentes de alta importancia.

19. Integridad de registros electrónicos

Los registros generados por los sistemas deberán contar con mecanismos para detectar modificaciones no autorizadas. El sistema deberá conservar:

- Usuario
- Fecha
- Hora
- Acción realizada
- Modificación
- Registro anterior cuando corresponda
- Registro posterior
- Cotivo de la modificación

Los operadores no deberán poder eliminar silenciosamente eventos relevantes.

20. Registro de accesos

Todo acceso a información sensible deberá quedar registrado. El sistema deberá poder responder, *quién accedió, cuándo accedió, qué consultó y qué acción realizó.* Esto permitirá investigar:

- Consultas indebidas
- Filtraciones
- Manipulación
- Accesos masivos
- Utilización de información para fines ajenos al servicio

21. Principio de necesidad de conocimiento

RD Propone RD Propone

El acceso deberá concederse conforme al principio de necesidad de conocimiento. Un funcionario no deberá tener acceso a toda la información simplemente por pertenecer a una determinada institución. El acceso deberá corresponder a:

- Función
- Responsabilidad
- Investigación
- Autorización
- Nivel de seguridad

La Ley 172-13 establece principios de licitud, calidad y seguridad en el tratamiento de datos personales, aunque contempla un régimen específico para archivos de organismos de investigación e inteligencia; el diseño del sistema deberá determinar cuidadosamente qué información queda dentro de cada régimen y qué controles son aplicables.

22. Calidad y corrección de la información

La inteligencia penitenciaria deberá basarse en información:

Pertinente;

- Verificable;
- Actualizada;
- Identificable;
- Contextualizada.

Un dato incorrecto puede generar una cadena de errores. Por ello, deberán existir procedimientos para:

- Corregir errores
- Incorporar información nueva
- Registrar contradicciones
- Diferenciar información confirmada de información no confirmada
- Identificar la fuente

El Tribunal Constitucional ha reconocido la importancia de los principios de calidad, licitud, lealtad y seguridad de los datos en materia de registros de inteligencia.

23. Clasificación de confiabilidad

La información de inteligencia deberá indicar, cuando resulte pertinente:

- Fuente

RD Propone RD Propone

- Fecha
- Nivel de confiabilidad
- Grado de corroboración
- Naturaleza de la información

De esta manera se evitará que una información preliminar sea tratada como un hecho comprobado.

24. Inteligencia humana

La tecnología no deberá sustituir completamente la inteligencia humana. Los informes podrán incorporar información proveniente de:

- Funcionarios
- Supervisores
- Entrevistas
- Investigaciones
- Denuncias
- Inspecciones
- Observaciones
- Fuentes institucionales autorizadas

Toda información deberá ser evaluada según su confiabilidad y finalidad.

25. Denuncias e información confidencial

El sistema deberá disponer de mecanismos para recibir información confidencial relacionada con:

- Introducción de dispositivos
- Corrupción
- Complicidad
- Amenazas
- Manipulación de sistemas
- Planificación delictiva

La información recibida deberá clasificarse como:

Alegación / *Información preliminar* / *Información corroborada* / *Evidencia*

Esta diferenciación evitará que una denuncia sin verificar sea tratada como una conclusión.

RD Propone RD Propone

26. Protección de fuentes

Cuando legalmente corresponda, deberán adoptarse medidas para proteger la identidad de las personas que suministren información sensible. La protección deberá incluir controles contra:

- Acceso no autorizado
- Filtración
- Represalias
- Divulgación interna innecesaria

Las reglas de protección deberán armonizarse con las obligaciones legales de investigación y debido proceso.

27. Inteligencia artificial como herramienta auxiliar

El sistema podrá utilizar inteligencia artificial para:

- Detectar patrones
- Identificar anomalías
- Priorizar alertas
- Analizar grandes volúmenes de registros
- Comparar eventos
- Identificar posibles relaciones
- Apoyar mantenimiento predictivo

Pero deberá aplicarse el principio, *la IA recomienda; la autoridad competente decide.* Una clasificación algorítmica no deberá ser suficiente por sí misma para imponer una sanción, realizar una imputación penal o adoptar una medida restrictiva de derechos.

28. Auditoría algorítmica

Cuando se utilicen modelos de inteligencia artificial, deberán mantenerse registros que permitan conocer:

- Qué sistema fue utilizado
- Qué versión
- Qué datos recibió
- Qué resultado produjo
- Quién revisó el resultado
- Qué decisión humana se tomó posteriormente

RD Propone RD Propone

Los modelos deberán evaluarse periódicamente para detectar:

- Errores
- Falsos positivos
- Falsos negativos
- Sesgos
- Degradación del rendimiento

29. Preservación de información

Cuando un evento pueda generar una investigación, deberán activarse mecanismos de preservación. Esto podrá incluir:

- Videos
- Registros de acceso
- Registros técnicos
- Fotografías
- Documentos
- Comunicaciones institucionales
- Registros de mantenimiento
- Información de operadores

La preservación deberá realizarse dentro de los plazos y procedimientos legalmente aplicables.

30. Información y prueba

El sistema deberá establecer una separación conceptual fundamental:

La inteligencia sirve para orientar la investigación; la prueba sirve para acreditar hechos dentro del procedimiento correspondiente.

Un informe de inteligencia puede justificar que se profundice una investigación, pero la responsabilidad penal o disciplinaria deberá establecerse mediante el procedimiento correspondiente y con respeto al debido proceso.

31. Coordinación con el Ministerio Público

Cuando los hechos puedan constituir delito, el sistema deberá activar el protocolo de comunicación con el Ministerio Público. La transferencia de información deberá documentar:

- Fecha

RD Propone RD Propone

- Institución que entrega
- Funcionario responsable
- Información entregada
- Soporte
- Motivo
- Identificación del incidente

Cuando corresponda, deberá preservarse el original y entregar una copia o representación técnicamente adecuada.

32. Coordinación con el Poder Judicial

Cuando una actuación requiera autorización judicial, la administración deberá contar con procedimientos claros para solicitarla. Esto será especialmente relevante respecto de medidas que impliquen afectación de derechos fundamentales.

El Tribunal Constitucional ha reiterado que la intervención de comunicaciones requiere autorización judicial competente y que la ausencia de dicha autorización puede generar nulidad de la medida y de las pruebas obtenidas.

33. Exclusión de evidencia obtenida irregularmente

Los protocolos deberán reconocer expresamente que la eficiencia investigativa no justifica obtener información mediante procedimientos contrarios a la Constitución o las leyes.

La evidencia obtenida mediante una actuación jurídicamente inválida podrá quedar sometida a las consecuencias procesales correspondientes. Este principio no debilita el sistema, por el contrario, obliga a diseñarlo correctamente desde el inicio.

34. Seguridad informática del sistema

La plataforma nacional deberá protegerse contra:

- Acceso no autorizado;
- Modificación;
- Eliminación;
- Extracción;
- Ransomware;
- Sabotaje;
- Manipulación interna;
- Ataques externos.

RD Propone RD Propone

Deberán establecerse:

- Autenticación robusta
- Segmentación de redes
- Registro de eventos
- Copias de respaldo
- Recuperación ante desastres
- Cifrado cuando corresponda
- Monitoreo
- Pruebas periódicas

35. Continuidad operacional

El sistema deberá mantener capacidades mínimas incluso ante:

- Interrupción eléctrica
- Caída de comunicaciones
- Falla de servidores
- Ataque cibernético
- Desastre natural
- Incendio
- Daño físico

Deberán existir procedimientos de contingencia. La pérdida temporal del sistema no deberá significar pérdida automática de los registros previamente generados.

36. Interoperabilidad institucional

Cuando legalmente proceda, los sistemas deberán permitir intercambio estructurado de información entre las instituciones participantes. La interoperabilidad deberá basarse en:

- Estándares
- Controles
- Perfiles de acceso
- Trazabilidad
- Autenticación
- Protocolos de intercambio

No deberá basarse en el intercambio informal de archivos mediante cuentas personales, aplicaciones no autorizadas o dispositivos removibles sin control.

37. Prohibición de bases de datos paralelas

RD Propone RD Propone

Ningún funcionario deberá crear bases de datos personales paralelas para almacenar información penitenciaria obtenida en el ejercicio de sus funciones.

Toda información oficial deberá permanecer dentro de sistemas institucionales autorizados. Esta regla será especialmente importante para evitar:

- Filtraciones
- Manipulación
- Pérdida de información
- Accesos no autorizados
- Desaparición de registros

38. Conservación y eliminación

La información no deberá conservarse indefinidamente sin fundamento. Deberán establecerse políticas de:

- Conservación
- Archivo
- Revisión
- Bloqueo
- Eliminación
- Anonimización cuando proceda

Los períodos de conservación deberán definirse conforme a la naturaleza de la información y las obligaciones legales aplicables.

39. Auditoría de inteligencia

El sistema deberá ser auditado periódicamente. Las auditorías deberán verificar:

- Quién accede
- Qué información consulta
- Si existe acceso injustificado
- Si se eliminan registros
- Si existen modificaciones
- Si se respetan los períodos de conservación
- Si los sistemas de IA funcionan adecuadamente
- Si se respetan los niveles de clasificación

40. Indicadores del sistema de inteligencia

RD Propone RD Propone

Deberán medirse, entre otros:

- Número de alertas
- Porcentaje de alertas confirmadas
- Falsos positivos
- Falsos negativos identificados
- Investigaciones generadas
- Incidentes prevenidos
- Tiempo de respuesta
- Reincidencia
- Vulnerabilidades detectadas
- Investigaciones concluidas
- Incidentes vinculados a corrupción
- Incidentes con evidencia suficiente
- Fallas de preservación

La calidad del sistema no deberá medirse por la cantidad de alertas producidas, sino por la utilidad y confiabilidad de sus resultados.

41. Informes nacionales

El Ministerio de Justicia deberá elaborar informes periódicos sobre:

- Tendencias
- Incidentes
- Vulnerabilidades
- Resultados
- Tecnología
- Investigaciones
- Medidas correctivas

La información publicada deberá ser agregada cuando la divulgación de detalles pueda comprometer la seguridad o investigaciones.

42. Evaluación independiente

Periódicamente deberá realizarse una evaluación independiente del sistema de información e inteligencia. La evaluación podrá revisar:

- Legalidad
- Seguridad

RD Propone RD Propone

- Precisión
- Eficiencia
- Costos
- Protección de datos
- Calidad de la inteligencia
- Utilidad para las investigaciones

Los resultados deberán utilizarse para introducir mejoras.

43. Principio de responsabilidad individual

Cada acceso, modificación, transferencia o utilización de información deberá poder asociarse a un usuario institucional. El anonimato operativo deberá quedar excluido. La regla deberá ser:

Si alguien puede acceder, el sistema debe poder registrar que accedió.

44. Integración con los capítulos anteriores

El Sistema Nacional de Información e Inteligencia deberá recibir información de:

Prevención → acceso → detección → monitoreo → alerta → respuesta → incautación → preservación → investigación → sanción → corrección.

Así, cada incidente deberá producir no solamente una respuesta inmediata, sino también conocimiento institucional.

45. Ciclo nacional de aprendizaje

Cada incidente relevante deberá generar una pregunta adicional:

¿Qué nos enseña este incidente sobre una vulnerabilidad que todavía existe?

El sistema deberá utilizar los resultados para modificar:

- Procedimientos
- Infraestructura
- Capacitación
- Tecnología
- Controles
- Horarios
- Supervisión
- Contratación

RD Propone RD Propone

- Protocolos

De esta forma, el sistema deberá aprender de sus propias fallas.

46. Principio de no utilización abusiva

La existencia de una arquitectura nacional de inteligencia penitenciaria no deberá interpretarse como autorización general para acumular información sobre las personas.

La información deberá ser:

Pertinente, necesaria, protegida, trazable y utilizada para una finalidad legítima.

La jurisprudencia constitucional reciente continúa desarrollando los límites relacionados con intimidad, autodeterminación informativa, hábeas data y registros de inteligencia.

47. Resultado esperado

Al finalizar la implementación del presente capítulo, el Estado deberá contar con una arquitectura capaz de pasar de **"encontramos un teléfono"** a:

"detectamos un evento → preservamos información → determinamos el contexto → identificamos la vulnerabilidad → activamos la investigación correspondiente → protegemos la evidencia → establecemos responsabilidades mediante el procedimiento aplicable → corregimos la vulnerabilidad."

Ese cambio representa uno de los principales objetivos estratégicos del programa.

CAPÍTULO XIX
RÉGIMEN ESPECIAL DE SEGURIDAD PARA FUNCIONARIOS, PROVEEDORES, CONTRATISTAS, VISITANTES Y TERCEROS

1. Objeto

El presente capítulo establece las medidas de control aplicables a las personas que, sin encontrarse privadas de libertad, ingresen, permanezcan, trabajen, presten servicios o desarrollen actividades dentro de los establecimientos penitenciarios.

Su finalidad será reducir el riesgo de que la cadena humana de acceso sea utilizada para:

- Introducir dispositivos electrónicos no autorizados
- Introducir tarjetas SIM u otros accesorios
- Introducir sustancias u objetos prohibidos
- Facilitar comunicaciones clandestinas

RD Propone RD Propone

- Manipular sistemas de seguridad
- Sustraer información
- Colaborar con actividades delictivas
- Evadir controles institucionales

El sistema deberá combinar prevención, control, trazabilidad, supervisión, investigación y responsabilidad.

2. Principio de control diferenciado

No todas las personas que ingresan a un establecimiento penitenciario presentan el mismo nivel de riesgo.

Por ello, el sistema deberá establecer categorías diferenciadas, tomando en consideración:

- Función;
- Frecuencia de ingreso;
- Nivel de acceso;
- Areas autorizadas;
- Naturaleza de la actividad;
- Duración de la permanencia;
- Acceso a sistemas;
- Acceso a población privada de libertad;
- Antecedentes de incidentes;
- Nivel de riesgo institucional.

El objetivo será evitar tanto los controles insuficientes como la aplicación indiscriminada de medidas excesivas.

3. Categorías de personas sujetas a control

El sistema deberá contemplar, como mínimo:

a. Personal penitenciario.
b. Personal administrativo.
c. Personal técnico.
d. Personal médico y sanitario.
e. Personal educativo y de reinserción.
f. Contratistas.
g. Proveedores.
h. Transportistas.

RD Propone RD Propone

i. Visitantes.
j. Abogados y representantes autorizados.
k. Representantes consulares.
l. Autoridades públicas.
m. Organizaciones autorizadas.
n. Personal de mantenimiento.
o. Personal de empresas de tecnología y telecomunicaciones.

Cada categoría deberá tener controles compatibles con su función y con las garantías jurídicas aplicables.

4. Identificación previa

Las personas que requieran acceso regular deberán contar con mecanismos de identificación institucional. Estos podrán incluir:

- Identificación oficial;
- Credencial institucional;
- Registro biométrico cuando legalmente proceda;
- Fotografía;
- Identificación de la institución o empresa;
- Autorización de acceso;
- Registro de áreas permitidas.

El sistema deberá evitar credenciales genéricas compartidas entre varias personas.

5. Principio de autorización previa

El acceso a zonas penitenciarias deberá estar basado en autorización previa, salvo las situaciones excepcionales establecidas legalmente. La autorización deberá indicar, cuando corresponda:

- Identidad
- Función
- Fecha
- Horario
- Establecimiento
- Area autorizada
- Motivo
- Persona responsable

RD Propone RD Propone

- Equipo autorizado

El simple hecho de pertenecer a una institución no deberá implicar acceso automático a todas las áreas penitenciarias.

6. Control de áreas

Los establecimientos deberán dividirse en zonas de seguridad. Como mínimo podrán establecerse:

Zona pública: áreas destinadas a atención, recepción y servicios.

Zona administrativa: oficinas y espacios de gestión.

Zona controlada: áreas con acceso restringido.

Zona crítica: áreas que contengan población privada de libertad, sistemas tecnológicos, infraestructura sensible o evidencia.

Zona altamente crítica: áreas cuyo acceso pueda comprometer gravemente la seguridad del establecimiento.

Cada zona deberá tener reglas específicas.

7. Principio de mínimo acceso necesario

Ningún funcionario, contratista o proveedor deberá tener acceso a una zona simplemente porque su función le permita ingresar al establecimiento. El acceso deberá limitarse a las áreas necesarias para realizar la tarea autorizada. Este principio deberá aplicarse especialmente a:

- Servidores
- Centros de monitoreo
- Cuartos de telecomunicaciones
- Sistemas eléctricos
- Almacenamiento de evidencia
- Depósitos
- Cámaras de seguridad
- Sistemas de control de acceso

8. Control de dispositivos electrónicos

RD Propone RD Propone

El establecimiento deberá establecer una política específica respecto de los dispositivos que puedan introducir funcionarios, proveedores, contratistas y visitantes. La política deberá determinar:

- Qué dispositivos están autorizados
- Cuáles están prohibidos
- Cuáles requieren registro
- Cuáles deben permanecer en áreas determinadas
- Qué dispositivos institucionales pueden utilizarse
- Cómo se documentan excepciones

No deberá existir una regla ambigua que permita a cada establecimiento interpretar de manera diferente qué puede entrar.

9. Registro de dispositivos autorizados

Cuando la naturaleza de una función requiera el ingreso de equipos electrónicos, deberá existir un registro institucional. Podrán registrarse:

- Teléfono
- Computadora
- Tableta
- Radio
- Herramienta electrónica
- Cámara
- Equipo especializado

El registro podrá incluir:

- Identificación del equipo;
- Responsable;
- Fecha de ingreso;
- Fecha de salida;
- Motivo;
- Area autorizada.

La finalidad será poder determinar posteriormente qué equipos estuvieron legítimamente dentro del establecimiento.

10. Equipos institucionales

RD Propone RD Propone

Cuando sea posible, deberán priorizarse dispositivos institucionales para funciones que requieran comunicación o acceso a información dentro de zonas sensibles. Estos equipos deberán contar con:

- Identificación
- Usuario individual
- Autenticación
- Registro de actividad
- Configuración de seguridad
- Administración remota cuando corresponda
- Mecanismos de bloqueo

Esto reducirá la dependencia de dispositivos personales dentro de áreas críticas.

11. Control de proveedores

Los proveedores deberán estar registrados previamente. El expediente deberá contener, según corresponda:

- Identificación de la empresa
- Identificación del personal
- Función
- Contrato
- Autorización
- Vehículo utilizado
- Equipos que ingresará
- Horario
- Area de trabajo
- Responsable institucional

Los proveedores no deberán poder sustituir libremente al personal autorizado sin notificación y actualización de registros.

12. Control de contratistas

Los contratos de servicios penitenciarios deberán incorporar cláusulas específicas de seguridad. Estas deberán contemplar:

- Obligación de cumplir protocolos
- Prohibición de introducir objetos no autorizados
- Deber de reportar incidentes

RD Propone RD Propone

- Controles de acceso
- Responsabilidad por personal subcontratado
- Protección de información
- Obligación de cooperación con auditorías
- Consecuencias contractuales
- Conservación de registros

La seguridad no deberá quedar fuera de los contratos como una materia exclusivamente administrativa.

13. Subcontratación

Ningún contratista podrá utilizar subcontratistas dentro del establecimiento sin autorización institucional cuando el contrato o la normativa así lo requiera. La empresa principal deberá mantener responsabilidad respecto del personal que utilice para ejecutar el servicio, conforme al contrato y al régimen jurídico aplicable.

Esto evitará que la subcontratación se convierta en un mecanismo para eludir controles.

14. Control de vehículos

Los vehículos que ingresen a los establecimientos deberán estar sujetos a procedimientos de control proporcionales al nivel de riesgo. Deberá registrarse:

- Matrícula
- Conductor
- Empresa
- Motivo
- Hora de entrada
- Hora de salida
- Carga
- Area autorizada

Cuando resulte técnicamente posible, los controles deberán permitir reconstruir posteriormente el recorrido del vehículo dentro del establecimiento.

15. Control de mercancías y herramientas

Las herramientas, materiales y mercancías deberán ingresar mediante procedimientos documentados. El sistema deberá permitir determinar:

- Qué ingresó

RD Propone RD Propone

- Quién lo introdujo
- Para qué se utilizará
- Dónde se utilizará
- Quién lo recibió
- Qué ocurrió con el material después de utilizarse

Las herramientas potencialmente reutilizables deberán estar sujetas a inventario cuando corresponda.

16. Control de equipos tecnológicos

Deberán utilizar procedimientos especiales, todos los técnicos encargados de instalar o mantener:

- cámaras;
- servidores;
- sistemas de detección;
- telecomunicaciones;
- redes;
- sistemas eléctricos;
- control de acceso;

Cada intervención deberá generar un registro que indique:

- Técnico
- Empresa
- Equipo intervenido
- Motivo
- Fecha
- Hora
- Cambios realizados
- Pruebas realizadas
- Autorización
- Responsable institucional

17. Principio de doble control

Las intervenciones sobre sistemas críticos deberán aplicar, cuando sea razonablemente posible, el principio de doble control. Por ejemplo:

Una persona realiza la intervención; otra verifica y documenta.

RD Propone RD Propone

Este mecanismo deberá aplicarse especialmente a:

- Servidores
- Almacenamiento de evidencia
- Sistemas de monitoreo
- Sistemas de telecomunicaciones
- Configuraciones críticas
- Sistemas eléctricos sensibles
- Controles de acceso

La finalidad será reducir el riesgo de manipulación individual no detectada.

18. Mantenimiento programado

Las intervenciones técnicas deberán programarse cuando sea posible. El establecimiento deberá conocer previamente:

- Quién ingresará
- Qué realizará
- Qué equipos llevará
- Cuánto tiempo permanecerá
- Qué sistemas serán intervenidos

Las intervenciones de emergencia deberán documentarse posteriormente con el mismo nivel de detalle.

19. Registro de entrada y salida

Toda persona que ingrese deberá quedar registrada de acuerdo con su categoría. El registro deberá permitir determinar:

Quién entró / Cuándo entró / Dónde estuvo autorizado a estar / Cuándo salió.

Este principio será esencial para las investigaciones posteriores.

20. Control de permanencia

El sistema deberá detectar, cuando técnicamente sea posible, situaciones como:

- Permanencia superior a la autorizada
- Acceso fuera de horario
- Ingreso a áreas no autorizadas
- Utilización de credenciales ajenas

RD Propone RD Propone

- Intentos repetidos de acceso

Una alerta deberá generar verificación humana antes de producir consecuencias.

21. Credenciales personales e intransferibles

Las credenciales de acceso deberán ser personales. Queda prohibido:

- Prestar credenciales
- Compartir contraseñas
- Utilizar credenciales de otra persona
- Mantener sesiones abiertas para terceros

Las infracciones deberán ser investigadas conforme al régimen correspondiente.

22. Supervisión aleatoria

Además de los controles ordinarios, podrán realizarse verificaciones aleatorias dentro del marco legal aplicable. Estas podrán incluir:

- Revisión de credenciales
- Verificación de equipos
- Inspección de áreas
- Verificación de inventarios
- Controles sobre vehículos
- Controles de herramientas

La selección aleatoria deberá contar con mecanismos que reduzcan la posibilidad de manipulación o discriminación.

23. Gestión de conflictos de interés

Los funcionarios y contratistas deberán declarar las situaciones de conflicto de interés que puedan comprometer su actuación. Deberán establecerse mecanismos para identificar:

- Relaciones económicas relevantes
- Vínculos contractuales
- Relaciones que puedan afectar la imparcialidad
- Situaciones de dependencia o influencia indebida

Cuando corresponda, deberán aplicarse mecanismos de separación funcional.

24. Rotación en funciones críticas

RD Propone RD Propone

Deberán estar sujetas a mecanismos de supervisión y, cuando resulte conveniente, rotación, las funciones que proporcionen acceso permanente a:

- Sistemas tecnológicos
- Inventarios
- Depósitos
- Areas críticas
- Información sensible
- Evidencia

La rotación deberá realizarse cuidadosamente para no afectar la especialización técnica necesaria.

25. Protección contra la corrupción

El sistema deberá identificar como riesgo específico la posibilidad de que funcionarios, contratistas o terceros colaboren deliberadamente con la introducción de dispositivos o con la vulneración de controles. Los mecanismos de prevención deberán incluir:

- Capacitación
- Supervisión
- Separación de funciones
- Controles aleatorios
- Auditorías
- Protección de denunciantes
- Investigación patrimonial cuando legalmente proceda
- Análisis de patrones
- Responsabilidad disciplinaria
- Responsabilidad penal cuando corresponda

26. Canal confidencial de denuncias

Deberá existir un mecanismo seguro para reportar:

- Introducción de dispositivos
- Solicitudes de soborno
- Amenazas
- Manipulación de controles
- Acceso irregular
- Filtración de información

RD Propone RD Propone

- Complicidad interna

El sistema deberá registrar la denuncia y establecer mecanismos para proteger la información de acuerdo con la ley.

27. Investigación de funcionarios y terceros

Cuando un incidente involucre a un funcionario, proveedor, visitante o contratista, la investigación deberá considerar toda la cadena de acceso. Deberá analizarse:

- Quién autorizó
- Quién ingresó
- Qué equipos llevaba
- Qué áreas visitó
- Cuánto tiempo permaneció
- Con quién tuvo contacto
- Qué controles atravesó
- Qué anomalías fueron registradas

La investigación no deberá limitarse a la persona que fue encontrada físicamente con el objeto.

28. Responsabilidad diferenciada

La responsabilidad deberá establecerse individualmente. Deberá diferenciarse entre:

- Conducta deliberada
- Complicidad
- Colaboración
- Beneficio económico
- Negligencia
- Omisión
- Error
- Incumplimiento de protocolo
- Falla sistémica

No toda falla de control deberá interpretarse automáticamente como corrupción.

29. Responsabilidad por omisión

RD Propone RD Propone

Cuando un funcionario tenga una obligación específica de control y deliberadamente omita cumplirla para facilitar una conducta ilícita, deberán activarse los mecanismos disciplinarios o penales que correspondan.

Deberá demostrarse la conducta y su relación con el hecho investigado.

La simple ocurrencia de un incidente no deberá generar responsabilidad automática del funcionario encargado.

30. Proveedores tecnológicos

Los contratos de proveedores que administren sistemas críticos deberán estar sujetos de las obligaciones especiales siguientes:

- Niveles de servicio
- Seguridad
- Confidencialidad
- Auditoría
- Registro de accesos
- Respuesta a incidentes
- Continuidad
- Respaldo
- Entrega de documentación
- Interoperabilidad
- Devolución de información
- Terminación ordenada del servicio

El Estado deberá evitar quedar técnicamente dependiente de un proveedor que sea el único capaz de comprender o mantener el sistema.

31. Acceso de proveedores a información

Los proveedores tecnológicos solo deberán acceder a la información estrictamente necesaria para prestar el servicio. Cuando sea posible, deberán utilizar:

- Cuentas temporales
- Accesos supervisados
- Registros de sesión
- Ambientes de prueba
- Información anonimizada

RD Propone RD Propone

El acceso remoto a sistemas críticos deberá estar sometido a controles especiales.

32. Derecho de abogados y representantes autorizados

Los controles de seguridad deberán aplicarse de manera compatible con las garantías correspondientes a abogados, representantes consulares y otras personas que ejerzan funciones protegidas por la ley.

La seguridad no deberá utilizarse como mecanismo para impedir injustificadamente la comunicación jurídica o consular.

Cuando existan procedimientos especiales de acceso, estos deberán encontrarse previamente definidos.

33. Visitantes

Los visitantes deberán recibir información clara sobre:

- Objetos prohibidos
- Dispositivos autorizados
- Reglas de ingreso
- Consecuencias de incumplimiento
- Mecanismos de reclamación

El visitante deberá poder conocer previamente las reglas aplicables.

34. Régimen de reincidencia

Cuando una persona que no se encuentre privada de libertad incumpla reiteradamente las reglas de acceso, podrán aplicarse las consecuencias administrativas, contractuales o legales que correspondan.

Cuando exista una prohibición de acceso, deberá encontrarse jurídicamente fundamentada y documentada.

35. Sistema de alertas de acceso

El sistema tecnológico podrá generar alertas ante:

- Credencial utilizada fuera de horario
- Acceso a zona no autorizada
- Credencial duplicada
- Permanencia anormal

RD Propone RD Propone

- Múltiples intentos de acceso
- Ingreso de equipos no registrados

Estas alertas deberán ser investigadas por personal competente, aunque una alerta tecnológica no deberá constituir por sí misma prueba de culpabilidad.

36. Integración con videovigilancia

Los sistemas de acceso deberán poder correlacionarse, cuando sea legal y técnicamente procedente, con los registros de videovigilancia. Esto permitirá verificar:

- Quién utilizó una credencial
- Dónde ocurrió el acceso
- Cuánto tiempo permaneció
- Qué personas lo acompañaron
- Si el registro coincide con las imágenes

La finalidad será mejorar la trazabilidad de los incidentes.

37. Auditoría de accesos

Las auditorías deberán buscar:

- Credenciales utilizadas por terceros
- Accesos fuera de horario
- Patrones inusuales
- Accesos repetidos
- Zonas con vulnerabilidades
- Discrepancias entre registros

Los resultados deberán incorporarse al sistema nacional de inteligencia penitenciaria.

38. Evaluación de empresas

Los proveedores y contratistas que participen en áreas críticas podrán estar sujetos a evaluación periódica de cumplimiento. La evaluación podrá considerar:

- Incidentes
- Cumplimiento contractual
- Capacitación
- Controles internos
- Seguridad de información
- Cooperación con auditorías

RD Propone RD Propone

- Mantenimiento
- Cumplimiento de protocolos

Los resultados deberán utilizarse conforme a la legislación de contratación pública.

39. Registro de incidentes de terceros

Todo incidente relacionado con un tercero deberá incorporarse al Registro Nacional de Incidentes cuando corresponda. Deberá poder determinarse:

- Persona
- Empresa
- Establecimiento
- Tipo de incidente
- Fecha
- Medida adoptada
- Resultado

La información deberá manejarse conforme al régimen de protección de datos aplicable.

40. Capacitación obligatoria

Toda persona que ingrese regularmente a zonas controladas deberá recibir capacitación adecuada a su función. Como mínimo deberá conocer:

- Objetos prohibidos
- Procedimientos de emergencia
- Reglas de acceso
- Protección de información
- Uso de dispositivos
- Obligación de reportar incidentes
- Consecuencias del incumplimiento

Los accesos deberán poder condicionarse, cuando corresponda, a la acreditación de dicha capacitación.

41. Certificación de personal crítico

El personal encargado de operar sistemas de monitoreo, telecomunicaciones, servidores, cámaras, controles de acceso, sistemas eléctricos críticos, deberá contar con capacitación y certificación institucional adecuadas.

42. Principio de trazabilidad humana

RD Propone RD Propone

Toda operación crítica deberá permitir reconstruir:

Quién la realizó / Con qué autorización / Cuándo / Sobre qué sistema / Qué modificó / Quién verificó

Este principio deberá convertirse en uno de los pilares del sistema.

43. Integración con el Centro Nacional de Monitoreo

Los incidentes relacionados con funcionarios, contratistas, proveedores y visitantes deberán poder incorporarse al Centro Nacional de Monitoreo cuando tengan relevancia para la seguridad. El Centro podrá correlacionarlos con:

- Dispositivos detectados
- Fallas de cámaras
- Accesos
- Incidentes anteriores
- Movimientos
- Mantenimiento
- Investigaciones

Esto permitirá detectar patrones que no serían visibles analizando cada incidente por separado.

44. Responsabilidad institucional

El sistema deberá reconocer que algunas vulnerabilidades no provienen exclusivamente de una persona. Una falla puede resultar de:

- falta de capacitación;
- procedimiento defectuoso;
- tecnología insuficiente;
- supervisión deficiente;
- diseño incorrecto;
- falta de mantenimiento;
- exceso de carga laboral;
- corrupción;
- negligencia;
- combinación de varios factores.

La investigación deberá determinar cuál de estos factores estuvo presente.

45. Prohibición de la cultura de encubrimiento

RD Propone RD Propone

Ningún funcionario deberá ser sancionado por reportar de buena fe una vulnerabilidad, falla o incidente simplemente porque la detección revele una deficiencia institucional. El sistema deberá distinguir entre:

"cometer una irregularidad y reportar una irregularidad"

Ocultar deliberadamente una vulnerabilidad deberá recibir un tratamiento diferente de informar oportunamente sobre ella.

46. Incentivos institucionales para reportar

La administración deberá promover una cultura en la cual reportar una falla, una vulnerabilidad, una conducta irregular, un intento de introducir un dispositivo, sea considerado parte de la responsabilidad profesional.

La seguridad no debe depender exclusivamente del miedo a ser sancionado, debe depender también de una cultura institucional de prevención.

47. Indicadores

El sistema deberá medir, entre otros:

- Número de personas autorizadas
- Cantidad de accesos
- Incidentes por categoría
- Dispositivos detectados en accesos
- Accesos irregulares
- Credenciales compartidas
- Incidentes de proveedores
- Incidentes de funcionarios
- Cumplimiento de capacitación
- Auditorías realizadas
- Investigaciones iniciadas
- Investigaciones concluidas
- Reincidencia
- Tiempo de respuesta

48. Evaluación periódica

Los protocolos de acceso deberán revisarse periódicamente. La revisión deberá determinar:

RD Propone RD Propone

- Qué controles funcionan
- Cuáles generan demoras innecesarias
- Dónde se producen vulnerabilidades
- Qué tecnologías necesitan actualización
- Qué categorías de personas presentan mayores riesgos
- Cuáles medidas deben modificarse

La seguridad deberá ser dinámica.

49. Principio de confianza controlada

El sistema penitenciario no deberá funcionar bajo la premisa de que toda persona que ingresa es una amenaza. Tampoco deberá funcionar bajo la premisa contraria de que toda persona autorizada es automáticamente confiable. El principio deberá ser:

La autorización permite el acceso; la trazabilidad permite confiar en el acceso.

La confianza institucional deberá estar acompañada de controles verificables.

50. Resultado esperado

La aplicación de este capítulo deberá permitir reducir significativamente uno de los riesgos estructurales del sistema penitenciario:

que una persona con acceso legítimo utilice ese acceso para facilitar una actividad ilegítima.

El modelo deberá permitir reconstruir cualquier incidente desde su origen:

Persona / Autorización / Ingreso / Equipo / Area / Permanencia / Interacción / Incidente / Investigación / Responsabilidad / Corrección.

De esta manera, el sistema dejará de concentrarse exclusivamente en descubrir el teléfono clandestino una vez dentro del establecimiento. La pregunta pasará a ser:

¿Cómo llegó allí, quién tuvo la oportunidad de introducirlo, qué controles atravesó, qué falló y qué debemos modificar para que vuelva a ocurrir?

Ese cambio convierte la seguridad penitenciaria de un sistema predominantemente reactivo en un sistema de *prevención, trazabilidad e inteligencia institucional.*

CAPÍTULO XX
RÉGIMEN NACIONAL DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD PENITENCIARIA

RD Propone RD Propone

1. Objeto

El presente capítulo establece el régimen nacional para la detección, validación, intervención, documentación, preservación de evidencias, investigación, corrección y cierre de incidentes de seguridad penitenciaria, con especial atención a aquellos relacionados con el ingreso, posesión, utilización, ocultamiento, suministro o facilitación de dispositivos electrónicos de comunicación no autorizados.

El régimen tendrá como finalidad asegurar que todo incidente sea atendido de manera:

1. Rápida
2. Proporcional
3. Documentada
4. Coordinada
5. Técnicamente verificable
6. Respetuosa de los derechos fundamentales
7. Orientada a la identificación de responsabilidades y
8. Dirigida a evitar la repetición del incidente

La respuesta institucional no deberá limitarse a la incautación del objeto detectado. Cada incidente deberá ser tratado como una fuente de información para determinar cómo ocurrió, quién pudo facilitarlo, qué controles fallaron y qué medidas deben adoptarse para impedir su repetición.

2. Principio de respuesta integral

Todo incidente de seguridad penitenciaria deberá ser gestionado mediante un proceso continuo compuesto, como mínimo, por las siguientes etapas:

ALERTA / VALIDACIÓN / CONTROL / PRESERVACIÓN / INTERVENCIÓN / DOCUMENTACIÓN / ESCALAMIENTO / INVESTIGACIÓN / DECISIÓN / CORRECCIÓN / CIERRE / APRENDIZAJE

La existencia de una alerta tecnológica no constituirá, por sí misma, prueba de responsabilidad individual. Toda decisión que pueda producir consecuencias disciplinarias, administrativas o penales deberá sustentarse en hechos verificables y en los procedimientos establecidos por la legislación aplicable.

3. Clasificación de los incidentes

Los incidentes deberán clasificarse según su naturaleza, alcance, riesgo y posible afectación a la seguridad.

RD Propone RD Propone

Se establecerán, como mínimo, las siguientes categorías:

a) Incidente tecnológico: Evento relacionado con cámaras, sensores, sistemas de detección, controles de acceso, redes, servidores, energía, comunicaciones u otros componentes tecnológicos.

b) Incidente de seguridad física: Evento relacionado con ingreso, ocultamiento, traslado, posesión o utilización de objetos prohibidos.

c) Incidente de comunicación no autorizada: Detección o confirmación de un dispositivo o mecanismo utilizado para establecer comunicaciones no autorizadas.

d) Incidente de integridad institucional: Evento que pueda involucrar a empleados, funcionarios, contratistas, proveedores, visitantes o terceros en la introducción, facilitación, ocultamiento o manipulación de elementos prohibidos.

e) Incidente criminal: Evento que presente elementos que puedan constituir una infracción penal o estar relacionado con la planificación, coordinación o ejecución de otros hechos delictivos.

f) Incidente crítico: Aquel que represente un riesgo inmediato o significativo para la vida, integridad física, seguridad del establecimiento, personal penitenciario, personas privadas de libertad, visitantes o terceros.

Un mismo hecho podrá pertenecer simultáneamente a más de una categoría.

4. Niveles de alerta

El Sistema Nacional establecerá una clasificación uniforme de alertas.

Nivel I - Alerta técnica: Anomalía tecnológica que requiere verificación.

Nivel II - Incidente confirmado: Evento comprobado que requiere intervención institucional ordinaria.

Nivel III - Incidente relevante: Evento que pueda comprometer varios controles o revelar una vulnerabilidad significativa.

Nivel IV - Incidente grave: Evento que pueda involucrar organización, complicidad interna, reiteración, amenaza directa o posible actividad criminal.

RD Propone RD Propone

Nivel V - Incidente crítico: Situación que represente riesgo inmediato para la vida, la seguridad del establecimiento o la población interna o externa, o que pueda estar vinculada con hechos criminales de especial gravedad.

La clasificación podrá modificarse durante la investigación cuando aparezcan nuevos elementos.

5. Detección

Las alertas podrán originarse mediante:

- Sistemas de detección tecnológica
- Cámaras de seguridad
- Controles de acceso
- Inspecciones ordinarias
- Inspecciones extraordinarias
- Registros de ingreso y salida
- Reportes del personal
- Denuncias o comunicaciones confidenciales
- Análisis de información
- Auditorías
- Mantenimiento técnico
- Investigaciones previas
- Información suministrada por otras instituciones públicas
- Información obtenida dentro de investigaciones legalmente autorizadas

Todo sistema tecnológico deberá permitir identificar, cuando resulte técnicamente posible:

- Fecha;
- Hora;
- Lugar;
- Sistema que generó la alerta;
- Operador que recibió la alerta;
- Actuación realizada;
- Resultado de la verificación.

6. Validación de la alerta

RD Propone RD Propone

La alerta deberá ser sometida a un proceso de validación humana que determine, si existe realmente un incidente, cuál es su naturaleza, cuál es su nivel de riesgo, qué área puede estar afectada, qué medidas inmediatas son necesarias y qué autoridades deben ser notificadas.

Los sistemas de inteligencia artificial podrán apoyar la detección de patrones o anomalías, pero la decisión institucional deberá permanecer bajo responsabilidad humana.

7. Control inicial del incidente

Una vez confirmado un incidente, el responsable del establecimiento deberá adoptar las medidas necesarias para:

- Proteger a las personas
- Controlar el área afectada
- Evitar la destrucción o alteración de evidencias
- Impedir que el incidente se extienda
- Preservar los registros tecnológicos
- Evitar interferencias innecesarias con otras actividades penitenciarias

Las medidas deberán ser proporcionales al riesgo existente.

No se permitirá utilizar una situación tecnológica menor como justificación para intervenciones generales, indiscriminadas o no relacionadas con el incidente.

8. Intervención proporcional

Toda intervención deberá ajustarse a los principios de:

- Legalidad
- Necesidad
- Proporcionalidad
- Mínima intervención
- Respeto a la dignidad humana
- Seguridad de las personas
- Preservación de evidencias

La intervención deberá orientarse a controlar el incidente, no a producir daños innecesarios a personas, bienes o infraestructura.

Particularmente, los mecanismos tecnológicos destinados a impedir comunicaciones no autorizadas deberán diseñarse de manera que no generen riesgos indebidos para otros

RD Propone RD Propone

sistemas esenciales del establecimiento, incluidos equipos médicos, sistemas de emergencia, comunicaciones institucionales, infraestructura eléctrica o mecanismos de seguridad.

9. Seguridad del personal y de las personas privadas de libertad

La respuesta ante un incidente deberá comenzar por la protección de la vida y la integridad física.

Cuando la naturaleza del incidente lo permita, deberán priorizarse mecanismos de control y contención que reduzcan riesgos innecesarios. El personal deberá recibir capacitación periódica para responder a:

- Incidentes tecnológicos
- Hallazgos de dispositivos
- Alteraciones de sistemas
- Situaciones de resistencia
- Emergencias
- Preservación de evidencia
- Comunicación de incidentes
- Protección de personas vulnerables

10. Preservación del área

Cuando exista posibilidad de que el incidente constituya evidencia de una infracción administrativa o penal, el área deberá preservarse de acuerdo con los protocolos institucionales. La preservación deberá procurar:

- Limitar accesos innecesarios
- Registrar quién ingresa
- Documentar cambios
- Preservar grabaciones
- Preservar registros electrónicos
- Conservar documentos relevantes
- Identificar posibles testigos
- Impedir manipulación o sustitución de objetos

La preservación deberá realizarse sin afectar innecesariamente las operaciones esenciales del establecimiento.

11. Preservación de sistemas tecnológicos

RD Propone RD Propone

Ante un incidente relevante, el responsable tecnológico deberá adoptar medidas para preservar, cuando corresponda:

- Grabaciones de cámaras
- Registros de acceso
- Registros de alarmas
- Registros de sistemas de detección
- Registros de operadores
- Bitácoras de mantenimiento
- Registros de configuración
- Registros de eventos
- Información de infraestructura tecnológica relacionada con el incidente

La información deberá conservarse de manera que pueda demostrarse posteriormente su integridad.

Queda prohibida la eliminación, alteración o sobrescritura deliberada de información relacionada con un incidente cuando exista obligación de preservarla.

12. Incautación de dispositivos

Cuando sea encontrado un teléfono móvil, tarjeta SIM, dispositivo electrónico u otro elemento prohibido, su tratamiento deberá realizarse conforme a un protocolo uniforme.

Deberá documentarse, cuando sea posible:

- Quién realizó el hallazgo
- Fecha y hora
- Ubicación
- Circunstancias del hallazgo
- Persona a quien se encontraba asociado, si corresponde
- Estado físico del objeto
- Identificación técnica disponible
- Fotografías
- Embalaje
- Persona que recibió el objeto
- Traslado
- Lugar de custodia

RD Propone RD Propone

La identificación técnica del dispositivo no deberá confundirse con el acceso a su contenido.

13. Prohibición de exploración informal del contenido

La incautación de un dispositivo no autoriza automáticamente a cualquier funcionario a revisar su contenido. El acceso a información almacenada en un dispositivo deberá sujetarse a las garantías constitucionales y legales aplicables, así como a las autorizaciones judiciales o fiscales que correspondan según la naturaleza de la actuación.

El personal penitenciario deberá limitarse a asegurar, identificar y preservar el dispositivo.

La extracción, análisis o utilización de información contenida en el dispositivo deberá corresponder a personal técnicamente autorizado y dentro del procedimiento legal aplicable.

14. Cadena de custodia

Todo elemento físico o digital que pueda constituir evidencia deberá incorporarse a una cadena de custodia verificable. La cadena deberá permitir reconstruir:

Hallazgo / Identificación / Embalaje / Recepción / Almacenamiento / Traslado / Análisis / Devolución o disposición final.

Cada transferencia deberá quedar registrada. La pérdida de trazabilidad deberá generar una investigación administrativa inmediata y, cuando corresponda, consecuencias conforme a la legislación aplicable.

15. Informe inicial de incidente

El informe deberá contener como mínimo:

1. Fecha y hora
2. Establecimiento
3. Area
4. Tipo de incidente
5. Mecanismo mediante el cual fue detectado
6. Personas involucradas o presentes
7. Acciones realizadas
8. Objetos encontrados

RD Propone RD Propone

9. Sistemas afectados
10. Evidencias preservadas
11. Funcionarios actuantes
12. Autoridades notificadas
13. Clasificación inicial del incidente
14. Medidas adoptadas

El informe inicial deberá realizarse aun cuando posteriormente se determine que el evento no constituyó una infracción.

16. Escalamiento institucional

Los incidentes ordinarios podrán ser gestionados por la administración del establecimiento.

Los incidentes relevantes deberán ser comunicados al nivel correspondiente de la Dirección General de Servicios Penitenciarios y Correccionales y al sistema nacional de monitoreo.

Los incidentes que puedan involucrar hechos criminales, corrupción, complicidad interna, amenazas graves o coordinación delictiva deberán activar los mecanismos de coordinación con el Ministerio de Justicia y el Ministerio Público, según corresponda.

La coordinación no deberá significar duplicación de funciones ni interferencia con las competencias legalmente atribuidas a cada institución.

17. Intervención del Ministerio Público

Cuando los hechos presenten características que puedan constituir una infracción penal, la autoridad penitenciaria deberá preservar la información disponible y comunicar el hecho a las autoridades competentes conforme al procedimiento establecido.

El Ministerio Público dirigirá las actuaciones de investigación penal que correspondan dentro de sus competencias constitucionales y legales.

La Constitución dominicana atribuye al Ministerio Público la dirección de la investigación penal y el ejercicio de la acción pública. La respuesta penitenciaria deberá, por tanto, distinguir claramente entre:

Seguridad penitenciaria / Investigación administrativa / Investigación penal

18. Autorizaciones judiciales

RD Propone RD Propone

Cuando una actuación de investigación requiera autorización judicial, esta deberá obtenerse mediante los mecanismos establecidos por la legislación vigente.

El sistema penitenciario no podrá sustituir al Poder Judicial ni utilizar mecanismos tecnológicos como vía indirecta para obtener información que legalmente requiera autorización. Este principio deberá incorporarse expresamente a los protocolos tecnológicos y operativos.

19. Investigación del origen del dispositivo

La investigación no deberá limitarse a determinar quién tenía el dispositivo al momento de su descubrimiento. Cuando existan elementos suficientes, deberá analizarse la cadena de posible introducción:

Origen / Adquisición / Transporte / Ingreso / Facilitación /+ Ocultamiento / Entrega / Posesión / Utilización.

La finalidad será determinar si existió:

- Introducción directa
- Facilitación
- Complicidad
- Omisión deliberada
- Corrupción
- Participación de terceros
- Participación de contratistas o proveedores
- Vulneración de controles
- Utilización de una falla tecnológica

20. Investigación de posibles patrones

Cuando existan incidentes repetidos, el Sistema Nacional deberá determinar si existe un patrón. Podrán analizarse, dentro del marco legal correspondiente:

- Horarios
- Areas
- Tipos de dispositivos
- Rutas de acceso
- Personal de servicio
- Proveedores

RD Propone RD Propone

- Visitantes
- Contratistas
- Fallas tecnológicas
- Eventos coincidentes
- Recurrencia de personas
- Recurrencia de dispositivos
- Vulnerabilidades comunes

El análisis de patrones tendrá carácter investigativo y preventivo y no podrá utilizarse para atribuir responsabilidad automáticamente a una persona.

21. Hipótesis de complicidad interna

Cuando las circunstancias indiquen una posible participación interna, deberá abrirse una línea específica de investigación. Esta deberá considerar, sin prejuzgar responsabilidades:

- Quién tuvo acceso al área
- Quién tenía autorización
- Quién realizó controles
- Quién manipuló sistemas
- Quién tuvo contacto con el objeto
- Quién efectuó mantenimiento
- Quién estuvo presente
- Qué registros existen
- Qué controles fallaron

La existencia de una coincidencia temporal o laboral no constituirá prueba suficiente de complicidad.

22. Participación de proveedores y terceros

Cuando el incidente pueda estar relacionado con un proveedor, contratista, visitante o tercero, deberán revisarse:

- Autorizaciones
- Registros de entrada y salida
- Vehículos
- Herramientas
- Equipos

RD Propone RD Propone

- Ordenes de trabajo
- Personal asignado
- Zonas visitadas
- Horarios
- Registros de mantenimiento
- Cámaras disponibles

Cuando corresponda, la institución podrá suspender preventivamente determinadas autorizaciones conforme al marco contractual y legal aplicable, sin convertir una medida preventiva en una declaración anticipada de culpabilidad.

23. Protección de posibles víctimas

Si durante una investigación surge información que indique una amenaza contra una persona, establecimiento o tercero, deberá activarse inmediatamente el protocolo de protección correspondiente. La prioridad será:

1. Preservar la vida
2. Controlar la amenaza
3. Proteger a la posible víctima
4. Preservar la evidencia
5. Comunicar a las autoridades competentes

La información sensible deberá manejarse bajo criterios de estricta necesidad y protección de datos.

24. Continuidad operacional

La respuesta a un incidente no deberá paralizar innecesariamente los servicios esenciales del establecimiento. Cada centro deberá contar con procedimientos de continuidad para:

- Comunicaciones institucionales
- Emergencias
- Atención médica
- Vigilancia
- Alimentación
- Acceso controlado
- Energía
- Sistemas informáticos
- Atención jurídica

RD Propone RD Propone

- Comunicaciones familiares legítimas

Cuando una medida de seguridad afecte temporalmente un servicio esencial, deberá existir un mecanismo alternativo autorizado.

25. Determinación de responsabilidades

Concluida la fase investigativa, deberán distinguirse claramente:

a) Responsabilidad penal
b) Responsabilidad administrativa
c) Responsabilidad disciplinaria
d) Responsabilidad contractual
e) Responsabilidad civil, cuando corresponda
f) Ausencia de responsabilidad

Una misma conducta podrá generar más de una consecuencia jurídica cuando el ordenamiento lo permita.

La determinación de responsabilidad deberá realizarse mediante la autoridad competente y respetando el debido proceso.

26. Prohibición de sanción basada exclusivamente en una alerta automatizada

Ninguna persona podrá ser sancionada exclusivamente porque:

- Un algoritmo haya generado una alerta
- Una cámara haya identificado una anomalía
- Un sistema haya detectado una posible señal
- Un patrón estadístico haya señalado una coincidencia

Las herramientas automatizadas deberán servir como mecanismos de detección, priorización y apoyo investigativo, nunca como sustitutos de la prueba y del procedimiento legal.

27. Análisis de causa raíz

Todo incidente relevante deberá concluir con un análisis de causa raíz, respondiendo:

1. ¿Qué ocurrió?
2. ¿Cuándo ocurrió?
3. ¿Dónde ocurrió?

RD Propone RD Propone

4. ¿Cómo pudo ocurrir?
5. ¿Qué control debía impedirlo?
6. ¿Por qué ese control no funcionó?
7. ¿Hubo una falla tecnológica?
8. ¿Hubo una falla humana?
9. ¿Hubo una falla organizacional?
10. ¿Hubo posible complicidad?
11. ¿Existe una vulnerabilidad que pueda repetirse?
12. ¿Qué medida concreta evitará la repetición?

El propósito será evitar que la respuesta institucional termine simplemente con la confiscación del objeto.

28. Plan de acciones correctivas

Cuando el análisis determine una vulnerabilidad, deberá generarse un plan de acción correctiva, identificando:

- Problema
- Causa
- Responsable
- Medida correctiva
- Presupuesto necesario
- Fecha límite
- Indicador de cumplimiento
- Mecanismo de verificación

Las acciones podrán incluir:

- Reparación tecnológica
- Modificación de procedimientos
- Capacitación
- Cambio de controles
- Rotación de funciones
- Revisión contractual
- Fortalecimiento de supervisión
- Modificación normativa
- Investigación adicional
- Actualización de software

RD Propone RD Propone

- Sustitución de equipos
- Refuerzo de infraestructura

29. Cierre del incidente

Un incidente solamente podrá declararse cerrado cuando:

1. Se haya controlado la situación
2. Se hayan preservado las evidencias necesarias
3. Se haya completado el informe
4. Se hayan realizado las notificaciones correspondientes
5. Se haya determinado la ruta administrativa o penal aplicable
6. Se hayan identificado las vulnerabilidades
7. Se hayan establecido las acciones correctivas
8. Se haya actualizado el registro nacional
9. Exista responsable de verificar las acciones pendientes

El cierre administrativo del incidente no impedirá que continúe una investigación penal cuando esta corresponda.

30. Base Nacional de Incidentes y Lecciones Aprendidas

Todos los incidentes relevantes deberán alimentar una base nacional destinada exclusivamente a:

- Prevención
- Análisis estadístico
- Identificación de patrones
- Evaluación tecnológica
- Auditoría
- Capacitación
- Planificación presupuestaria
- Mejora institucional

La información deberá clasificarse según su nivel de sensibilidad.

La publicación de estadísticas deberá evitar la exposición de información que pueda comprometer investigaciones, operaciones de seguridad o derechos de las personas.

31. Evaluación posterior al incidente

Los incidentes de niveles IV y V deberán generar una evaluación posterior obligatoria.

RD Propone RD Propone

La evaluación deberá realizarse independientemente de que posteriormente exista o no una condena penal.

20.32. Indicadores de respuesta

El Sistema Nacional deberá medir, entre otros:

Tiempo de detección: tiempo transcurrido entre la ocurrencia estimada del evento y su identificación.

Tiempo de validación: tiempo entre la alerta y la confirmación humana.

Tiempo de respuesta: tiempo entre la confirmación y la intervención.

Tiempo de preservación: tiempo necesario para asegurar las evidencias relevantes.

Tiempo de escalamiento: tiempo entre la clasificación del incidente y la notificación a la autoridad correspondiente.

Tiempo de cierre: tiempo requerido para completar la gestión administrativa del incidente.

Tasa de reincidencia: porcentaje de incidentes que vuelven a producirse en condiciones similares.

Tasa de corrección: porcentaje de vulnerabilidades identificadas que fueron efectivamente corregidas.

33. Pruebas y simulaciones

Los establecimientos deberán realizar periódicamente ejercicios controlados destinados a comprobar:

- Detección
- Comunicación
- Reacción
- Coordinación
- Preservación de evidencia
- Continuidad
- Documentación
- Escalamiento

RD Propone RD Propone

- Funcionamiento de los sistemas tecnológicos

Los ejercicios deberán diseñarse de forma que no revelen públicamente vulnerabilidades específicas de los establecimientos.

Cada ejercicio deberá producir un informe de resultados y un plan de mejora.

34. Responsabilidad del mando

Los responsables de cada nivel deberán conocer sus obligaciones ante un incidente. La ausencia de actuación, la ocultación deliberada de un evento, la destrucción de evidencia o la alteración intencional de registros deberán generar las consecuencias previstas por el ordenamiento jurídico.

Sin embargo, no deberá confundirse una deficiencia institucional o una falla tecnológica con responsabilidad individual automática.

La investigación deberá determinar las circunstancias concretas de cada caso.

35. Transparencia y reserva

El Estado deberá publicar periódicamente información estadística sobre:

- Cantidad de incidentes
- Tipos de incidentes
- Dispositivos incautados
- Establecimientos afectados
- Tiempos de respuesta
- Acciones correctivas
- Resultados de auditorías
- Evolución de indicadores

No deberán publicarse detalles técnicos cuya divulgación facilite la evasión de controles, comprometa investigaciones o exponga vulnerabilidades de seguridad.

De esta manera se establece un equilibrio entre:

transparencia pública + seguridad institucional + protección de derechos.

36. Integración con el Sistema Nacional de Seguridad Penitenciaria

El régimen de respuesta deberá integrarse con el Sistema Nacional de Monitoreo, el sistema de inteligencia penitenciaria, los controles de acceso, el sistema de videovigilancia, los sistemas tecnológicos de detección, el registro de incidentes, los

RD Propone RD Propone

mecanismos de auditoría, el régimen disciplinario, los protocolos de coordinación con el Ministerio Público y los mecanismos de coordinación tecnológica con las instituciones competentes.

La finalidad será evitar que cada establecimiento gestione los incidentes como hechos aislados.

37. Principio de aprendizaje institucional

Cada incidente deberá producir conocimiento útil para prevenir el siguiente. Por tanto, el sistema deberá pasar de una lógica exclusivamente reactiva *"ocurrió / incautamos / sancionamos"* a una lógica de seguridad permanente:

"ocurrió / detectamos / controlamos / preservamos / investigamos / determinamos responsabilidades / identificamos la causa / corregimos / verificamos / aprendemos"

Este principio deberá orientar todo el Sistema Nacional.

38. Resultado esperado

El régimen nacional de respuesta deberá lograr que ningún incidente relevante termine simplemente archivado como una incautación aislada.

Cada evento deberá permitir responder, con el mayor grado posible de certeza:

qué ocurrió, cómo ocurrió, dónde ocurrió, cuándo ocurrió, qué controles fallaron, quiénes tuvieron acceso, qué evidencia existe, qué responsabilidades pueden derivarse, qué vulnerabilidad fue descubierta y qué se hizo para evitar que vuelva a ocurrir.

CAPÍTULO XXI
PROTECCIÓN DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD TECNOLÓGICA DEL SISTEMA PENITENCIARIO

21.1. Objeto

El presente capítulo establece las disposiciones generales destinadas a proteger la información, los sistemas tecnológicos, las comunicaciones institucionales, las bases de datos, los registros electrónicos, los dispositivos de seguridad y demás activos digitales que formen parte del Sistema Nacional de Seguridad Penitenciaria. Su finalidad será garantizar:

1. Confidencialidad
2. Integridad

RD Propone RD Propone

3. Disponibilidad
4. Autenticidad
5. Trazabilidad
6. Continuidad operacional
7. Recuperación ante incidentes
8. Protección de los derechos fundamentales

La seguridad tecnológica deberá ser considerada parte integral de la seguridad penitenciaria y no un componente meramente informático.

2. Principio de seguridad por diseño

Todo sistema tecnológico que se incorpore al Sistema Nacional deberá diseñarse desde el inicio considerando sus riesgos de seguridad. No deberá adquirirse una tecnología únicamente porque cumpla una función operativa.

Antes de su implementación deberá evaluarse, como mínimo:

- Qué información manejará
- Quién podrá acceder
- Dónde estará almacenada
- Cómo será protegida
- Qué ocurrirá si falla
- Cómo podrá recuperarse
- Cómo se auditarán sus operaciones
- Cómo se actualizará
- Quién será responsable
- Qué dependencia tecnológica generará
- Cómo se retirará al finalizar su vida útil

La seguridad deberá formar parte de las especificaciones técnicas, contratos, pruebas de aceptación y procesos de mantenimiento.

3. Inventario nacional de activos tecnológicos

El Sistema Nacional deberá mantener un inventario actualizado de los activos tecnológicos críticos. El inventario deberá incluir, según corresponda:

- Cámaras
- Servidores
- Sistemas de almacenamiento

RD Propone RD Propone

- Equipos de red
- Sistemas de control de acceso
- Sensores
- Sistemas de detección
- Estaciones de monitoreo
- Sistemas de comunicaciones
- Dispositivos institucionales
- Sistemas de respaldo
- Software
- Bases de datos
- Sistemas de alimentación eléctrica asociados
- Infraestructura de telecomunicaciones
- Equipos de respaldo
- Licencias y certificados digitales

Cada activo crítico deberá tener:

- Identificación única
- Ubicación
- Responsable
- Función
- Fabricante
- Modelo
- Versión
- Fecha de instalación
- Estado
- Fecha de mantenimiento
- Nivel de criticidad

4. Clasificación de la información

La información generada por el sistema deberá clasificarse de acuerdo con su sensibilidad. Se establecerán, como mínimo:

Nivel I - Información pública: Información que pueda ser divulgada sin comprometer la seguridad.

Nivel II - Información institucional: Información de uso interno cuya divulgación no autorizada pueda afectar la operación administrativa.

RD Propone RD Propone

Nivel III - Información sensible: Información cuya divulgación pueda comprometer la seguridad, investigaciones, personas o infraestructura.

Nivel IV - Información crítica o reservada: Información cuya divulgación pueda generar un riesgo significativo para operaciones de seguridad, investigaciones criminales, infraestructura crítica, personas protegidas o sistemas tecnológicos.

La clasificación no deberá utilizarse para ocultar información que legalmente deba ser pública.

5. Acceso basado en funciones

Ningún funcionario deberá disponer de acceso generalizado a todos los sistemas. Se aplicarán los principios de "necesidad de saber" y "mínimo privilegio".

Una persona que tenga autorización para observar cámaras no deberá tener automáticamente autorización para:

- Modificar configuraciones
- Extraer información
- Administrar bases de datos
- Eliminar registros
- Acceder a investigaciones
- Administrar sistemas de comunicaciones

Las funciones críticas deberán mantenerse separadas cuando sea técnicamente posible.

6. Identidad digital de los usuarios

Todo usuario con acceso a sistemas críticos deberá disponer de una identidad digital individual. Queda prohibido:

- Compartir credenciales
- Utilizar cuentas genéricas para funciones críticas
- Permitir el uso de una cuenta por otra persona
- Almacenar contraseñas de manera insegura
- Mantener accesos de funcionarios que ya no desempeñen las funciones correspondientes

Los accesos deberán ser:

- Autorizados
- Registrados

RD Propone RD Propone

- Revisables
- Revocables
- Auditables

Cuando la criticidad del sistema lo justifique, deberá utilizarse autenticación multifactor.

7. Administración de privilegios

El sistema deberá contemplar:

- Altas
- Modificaciones
- Suspensiones
- Revocaciones
- Accesos temporales
- Accesos extraordinarios
- Accesos de emergencia

Cuando un funcionario sea trasladado, suspendido, separado de sus funciones o cambie de responsabilidad, sus permisos deberán ser revisados inmediatamente. La permanencia de privilegios innecesarios deberá considerarse una vulnerabilidad institucional.

8. Registro de actividad

Los sistemas críticos deberán generar registros que permitan determinar, cuando corresponda:

- Quién accedió
- Cuándo accedió
- Desde dónde
- Qué función ejecutó
- Qué información consultó
- Qué modificación realizó
- Qué información exportó
- Qué sistema utilizó

Los registros de auditoría deberán contar con mecanismos que dificulten su alteración no autorizada. La eliminación deliberada o manipulación de registros de seguridad deberá generar una investigación.

9. Protección de bases de datos

RD Propone RD Propone

Las bases de datos que contengan información penitenciaria deberán contar con mecanismos de protección apropiados a su nivel de sensibilidad. Deberán establecerse medidas para:

- evitar accesos no autorizados;
- Evitar alteraciones
- Prevenir pérdida de información
- Mantener respaldos
- Verificar integridad
- Controlar exportaciones
- Detectar accesos anómalos
- Recuperar información

No deberá existir una única copia de información crítica.

10. Cifrado y protección de información sensible

La información sensible deberá protegerse mediante mecanismos técnicos adecuados, incluyendo cifrado cuando corresponda. La protección deberá aplicarse tanto a la información almacenada como a aquella que sea transmitida por redes no confiables.

Las claves criptográficas deberán administrarse mediante procedimientos institucionales y no depender de una sola persona. La pérdida o exposición de una clave crítica deberá activar un procedimiento de respuesta.

11. Comunicaciones institucionales

Las comunicaciones utilizadas para seguridad penitenciaria deberán contar con mecanismos destinados a protegerlas frente a:

- Interceptación no autorizada
- Manipulación
- Suplantación
- Pérdida
- Indisponibilidad
- Alteración

Las redes utilizadas para sistemas críticos deberán mantenerse separadas, física o lógicamente, de redes destinadas a usos ordinarios cuando la evaluación de riesgo así lo determine.

RD Propone RD Propone

12. Segmentación de sistemas

La arquitectura tecnológica deberá evitar que una vulnerabilidad en un sistema comprometa automáticamente todos los demás. Los sistemas deberán segmentarse según su función y criticidad.

Como principio general, deberá evitarse que:

Una cámara comprometida / permita comprometer el control de acceso;
un equipo administrativo comprometido / permita acceder al sistema de seguridad;
una cuenta ordinaria / permita administrar infraestructura crítica.

La arquitectura deberá diseñarse bajo el principio de defensa en profundidad.

13. Protección de cámaras y videovigilancia

Las cámaras constituirán infraestructura crítica de seguridad y deberán contar con mecanismos para:

- Controlar acceso
- Proteger grabaciones
- Detectar interrupciones
- Identificar pérdida de señal
- Detectar alteraciones
- Registrar mantenimiento
- Proteger configuración
- Verificar disponibilidad

El sistema deberá generar alertas cuando una cámara crítica quede fuera de servicio de manera no programada. No deberá considerarse normal una interrupción prolongada de un sistema de videovigilancia crítico.

14. Integridad de las grabaciones

Las grabaciones relacionadas con incidentes deberán conservar mecanismos que permitan verificar razonablemente:

- Origen
- Fecha
- Hora
- Integridad
- Período de almacenamiento

RD Propone RD Propone

- Acceso
- Copia
- Transferencia

La extracción de una grabación relevante deberá quedar registrada. Cuando una grabación sea incorporada como evidencia, deberá aplicarse el régimen de preservación y cadena de custodia correspondiente.

15. Protección de sistemas de detección

Los sistemas utilizados para detectar dispositivos, anomalías o actividades no autorizadas deberán protegerse contra:

- Manipulación
- Desactivación
- Modificación
- Acceso no autorizado
- Alteración de parámetros
- Introducción de información falsa

Toda modificación de parámetros críticos deberá generar un registro. Cuando sea posible, las modificaciones deberán requerir autorización diferenciada y quedar sujetas a auditoría.

16. Protección de los sistemas de control de acceso

Deberán contar con mecanismos de seguridad adecuados, los sistemas que administren:

- Puertas
- Credenciales
- Zonas restringidas
- Autorizaciones
- Horarios
- Visitantes
- Vehículos

Las acciones administrativas sobre estos sistemas deberán quedar registradas. Los accesos de emergencia deberán estar especialmente auditados.

17. Seguridad de proveedores tecnológicos

RD Propone RD Propone

Todo proveedor que tenga acceso a sistemas críticos deberá cumplir requisitos de seguridad definidos contractualmente. Los contratos deberán contemplar, según corresponda:

- Confidencialidad
- Protección de información
- Control de acceso
- Registro de actividades
- Notificación de incidentes
- Obligaciones de mantenimiento
- Eliminación o devolución de información
- Continuidad
- Soporte
- Actualización
- Gestión de vulnerabilidades
- Cooperación en investigaciones
- Responsabilidad por incumplimiento

El proveedor no deberá convertirse en administrador permanente e ilimitado de los sistemas del Estado.

18. Acceso remoto de proveedores

El acceso remoto a infraestructura penitenciaria crítica deberá ser:

- Autorizado
- Limitado
- Temporal cuando sea posible
- Registrado
- Supervisado
- Revocable

Cuando una intervención remota termine, el acceso deberá cerrarse. Los accesos extraordinarios deberán quedar identificados para posteriores auditorías.

19. Actualizaciones y gestión de vulnerabilidades

Los sistemas tecnológicos deberán mantenerse actualizados de acuerdo con las recomendaciones técnicas del fabricante y la evaluación de riesgo institucional. La actualización deberá considerar:

RD Propone RD Propone

- Pruebas previas
- Compatibilidad
- Respaldo
- Ventana de mantenimiento
- Plan de reversión
- Verificación posterior

No deberá instalarse una actualización directamente sobre un sistema crítico sin evaluar previamente sus posibles efectos.

20. Gestión de vulnerabilidades

El Sistema Nacional deberá establecer un proceso permanente para identificar y corregir vulnerabilidades. Las vulnerabilidades deberán clasificarse según:

- Gravedad
- Posibilidad de explotación
- Impacto
- Exposición
- Criticidad del sistema

Las vulnerabilidades críticas deberán recibir tratamiento prioritario. El sistema deberá mantener un registro de:

Vulnerabilidad / Responsable / Acción / Fecha prevista / Corrección / Verificación

21. Pruebas de seguridad

Los sistemas críticos deberán someterse periódicamente a pruebas de seguridad. Dichas pruebas podrán incluir:

- Revisión de configuración
- Análisis de vulnerabilidades
- Auditorías
- Pruebas controladas
- Revisión de accesos
- Verificación de respaldos
- Pruebas de recuperación
- Ejercicios de respuesta

Las pruebas deberán realizarse bajo autorización institucional y sin poner innecesariamente en riesgo los sistemas operativos.

RD Propone RD Propone

22. Detección de incidentes cibernéticos

El Sistema Nacional deberá disponer de mecanismos para detectar:

- accesos anómalos;
- intentos reiterados de acceso;
- modificación no autorizada;
- pérdida de información;
- malware;
- indisponibilidad;
- alteración de registros;
- conexiones inusuales;
- comportamiento anómalo.

Cuando exista evidencia suficiente de un incidente, deberá activarse el régimen nacional de respuesta establecido en el Capítulo XX.

23. Respuesta ante incidentes cibernéticos

Ante un incidente tecnológico, la respuesta deberá procurar:

1. Detectar
2. Validar
3. Contener
4. Preservar
5. Investigar
6. Recuperar
7. Corregir
8. Documentar
9. Aprender

La respuesta deberá distinguir entre un *incidente técnico accidental, incidente provocado deliberadamente, fallo de proveedor, error humano, y posible ataque criminal.*

24. Continuidad operacional

Cada establecimiento deberá contar con un plan de continuidad tecnológica, el cual deberá determinar qué servicios son críticos y cómo continuarán funcionando ante:

- Pérdida de energía
- Caída de redes

RD Propone RD Propone

- Fallo de servidores
- Daño físico
- Ataque cibernético
- Incendio
- Inundación
- Desastre natural
- Pérdida de conectividad
- Indisponibilidad de un proveedor

La continuidad deberá priorizar:

1. Vida y seguridad
2. Comunicaciones de emergencia
3. Vigilancia
4. Control de acceso
5. Atención médica
6. Comunicaciones institucionales
7. Sistemas de información esenciales

25. Sistemas de respaldo

Los sistemas críticos deberán contar con mecanismos de respaldo adecuados. Los respaldos deberán:

- Realizarse periódicamente
- Protegerse contra alteraciones
- Mantenerse separados del sistema principal
- Ser sometidos a pruebas
- Contar con procedimientos de recuperación

Un respaldo que nunca haya sido probado no deberá considerarse garantía suficiente de recuperación.

26. Recuperación ante desastres

El Sistema Nacional deberá establecer procedimientos para recuperar progresivamente los servicios tecnológicos después de un evento grave. Cada sistema crítico deberá contar, según corresponda, con:

- Prioridad de recuperación
- Responsable

RD Propone RD Propone

- Tiempo objetivo de recuperación
- Información que debe recuperarse
- Procedimiento alternativo
- Mecanismo de verificación

La recuperación deberá ser probada periódicamente.

27. Protección de la infraestructura eléctrica y física

La infraestructura eléctrica que soporte sistemas críticos deberá contar con medidas de protección, respaldo y supervisión. El propósito será garantizar:

- Continuidad
- Seguridad
- Estabilidad
- Protección de equipos
- Detección de anomalías

No deberá utilizarse deliberadamente la infraestructura eléctrica de los establecimientos como mecanismo para dañar, destruir o inutilizar dispositivos electrónicos personales. Las medidas tecnológicas deberán orientarse a la detección, control y prevención, no a la generación deliberada de daños colaterales.

28. Independencia y redundancia

Los sistemas críticos no deberán depender de un único punto de falla cuando la evaluación de riesgo determine que dicha dependencia compromete la seguridad. Deberán evaluarse mecanismos de:

- Redundancia
- Respaldo
- Comunicaciones alternativas
- Almacenamiento alternativo
- Energía de respaldo
- Recuperación

La redundancia deberá aplicarse de manera proporcional al nivel de criticidad y al presupuesto disponible.

29. Dependencia tecnológica de proveedores

RD Propone RD Propone

Las adquisiciones deberán evitar situaciones en las que un único proveedor tenga control exclusivo sobre:

- Datos
- Configuraciones
- Códigos
- Infraestructura
- Licencias
- Mantenimiento
- Recuperación

Los contratos deberán establecer mecanismos de continuidad y transferencia. Cuando sea técnicamente posible, deberán utilizarse estándares abiertos e interoperables.

30. Portabilidad de la información

La información institucional deberá poder ser transferida a otro sistema cuando sea necesario, conforme a las condiciones técnicas y legales aplicables.

El Estado no deberá quedar imposibilitado de migrar información porque un proveedor haya utilizado formatos propietarios sin mecanismos adecuados de exportación.

31. Protección de datos personales

El tratamiento de datos personales deberá respetar el marco jurídico aplicable. La información deberá ser:

- Obtenida para una finalidad legítima
- Pertinente
- Adecuada
- Protegida
- Utilizada conforme a su finalidad
- Accesible solamente a quienes corresponda

La existencia de una infraestructura de seguridad no constituye autorización para recolectar información ilimitada sobre todas las personas. Deberá existir una relación razonable entre:

Información recopilada / Finalidad de seguridad / Necesidad / Protección

RD Propone RD Propone

La Ley 172-13 establece principios de licitud y calidad del tratamiento de datos personales y regula el uso de estos datos en bancos de información, con reglas especiales para determinados archivos de investigación e inteligencia.

32. Retención y eliminación

Cada categoría deberá contar con reglas de conservación acordes con:

- Finalidad
- Naturaleza
- Valor probatorio
- Obligaciones legales
- Necesidades de seguridad
- Investigaciones
- Auditorías

Cuando concluya el período aplicable y no exista fundamento legal para conservar la información, deberá procederse conforme a los mecanismos establecidos para su eliminación o anonimización, según corresponda.

33. Información utilizada para inteligencia

La información utilizada para inteligencia penitenciaria deberá estar sujeta a controles especiales, registrando:

- Origen
- Fecha
- Nivel de confiabilidad
- Finalidad
- Acceso
- Utilización
- Período de conservación

La información de inteligencia no deberá convertirse automáticamente en prueba ni en fundamento exclusivo de una sanción.

34. Inteligencia artificial y sistemas automatizados

Los sistemas de inteligencia artificial podrán utilizarse como herramientas auxiliares para:

- Detectar anomalías

RD Propone RD Propone

- Identificar patrones
- Priorizar alertas
- Analizar grandes volúmenes de información
- Apoyar auditorías
- Identificar posibles fallas

Sin embargo:

Ninguna decisión que afecte derechos fundamentales deberá basarse exclusivamente en una conclusión automatizada.

Deberán existir:

- Supervisión humana
- Registros
- Posibilidad de revisión
- Evaluación de errores
- Auditoría
- Control de acceso
- Protección contra manipulación

35. Seguridad de los sistemas de inteligencia artificial

Cuando se utilicen herramientas de inteligencia artificial deberán evaluarse riesgos como:

- Datos incorrectos
- Resultados falsos
- Sesgos
- Manipulación
- Contaminación de datos
- Errores de clasificación
- Dependencia excesiva del sistema

Los modelos deberán ser evaluados periódicamente. El personal deberá conocer las limitaciones de estas herramientas.

36. Formación del personal

Todo personal con acceso a sistemas tecnológicos críticos deberá recibir capacitación periódica. La capacitación deberá incluir:

- Seguridad digital

RD Propone RD Propone

- Protección de contraseñas
- Identificación de intentos de fraude
- Manejo de información sensible
- Respuesta ante incidentes
- Protección de evidencia
- Uso correcto de sistemas
- Obligaciones de confidencialidad
- Consecuencias de la manipulación de registros

La seguridad tecnológica no deberá depender exclusivamente del departamento de informática.

37. Cultura institucional de ciberseguridad

La seguridad tecnológica deberá convertirse en una responsabilidad institucional compartida. Cada funcionario deberá comprender que:

> *Una contraseña compartida, una cuenta sin revocar, un registro eliminado o una computadora conectada indebidamente pueden convertirse en una vulnerabilidad de seguridad penitenciaria.*

La institución deberá promover una cultura de prevención y reporte temprano.

38. Canal de reporte de vulnerabilidades

Deberá existir un mecanismo institucional para reportar:

- Fallas;
- Vulnerabilidades;
- Accesos indebidos;
- Pérdida de información;
- Comportamientos sospechosos;
- Fallos de sistemas;
- Problemas de continuidad.

Los reportes realizados de buena fe deberán ser evaluados sin generar represalias por el simple hecho de comunicar una vulnerabilidad. Cuando existan indicios de conducta deliberadamente dañina, se aplicarán los procedimientos correspondientes.

39. Auditoría tecnológica independiente

La auditoría deberá revisar:

- Accesos

RD Propone RD Propone

- Configuraciones
- Vulnerabilidades
- Respaldos
- Continuidad
- Proveedores
- Registros
- Cumplimiento de políticas
- Incidentes
- Correcciones

La auditoría deberá tener independencia funcional suficiente para producir hallazgos confiables.

40. Certificación de sistemas críticos

Antes de poner en funcionamiento un sistema crítico deberá verificarse:

1. Cumplimiento de especificaciones
2. Seguridad
3. Funcionamiento
4. Integración
5. Respaldo
6. Recuperación
7. Trazabilidad
8. Capacitación
9. Documentación
10. Aceptación institucional

Ningún sistema crítico deberá considerarse plenamente operativo únicamente porque el proveedor haya declarado terminada su instalación.

41. Pruebas antes de la puesta en servicio

Deberá verificarse, como mínimo:

- Funcionamiento normal
- Funcionamiento bajo carga
- Pérdida de conectividad
- Pérdida de energía
- Recuperación

RD Propone RD Propone

- Respaldo
- Alarmas
- Registros
- Controles de acceso
- Interoperabilidad

Las deficiencias críticas deberán corregirse antes de la entrada en producción.

42. Registro Nacional de Incidentes Tecnológicos

Este registro deberá permitir conocer:

- Tipo de incidente
- Sistema afectado
- Fecha
- Establecimiento
- Causa
- Impacto
- Tiempo de recuperación
- Proveedor involucrado
- Medida correctiva
- Reincidencia

Este registro permitirá determinar si determinados equipos, proveedores o tecnologías presentan patrones de fallas.

43. Indicadores de ciberseguridad y continuidad

Deberán establecerse, entre otros, los siguientes indicadores:

- Disponibilidad de sistemas críticos
- Porcentaje de sistemas con respaldo probado
- Porcentaje de usuarios con autenticación reforzada
- Cantidad de accesos indebidos
- Vulnerabilidades críticas pendientes
- Tiempo promedio de corrección
- Tiempo de recuperación
- Cantidad de incidentes cibernéticos
- Porcentaje de sistemas auditados
- Porcentaje de personal capacitado

RD Propone RD Propone

- Cantidad de cuentas revocadas oportunamente
- Porcentaje de proveedores evaluados

44. Evaluación periódica

El Sistema Nacional deberá evaluar anualmente la madurez tecnológica de cada establecimiento. La evaluación deberá considerar:

personas + procesos + tecnología + información + infraestructura + continuidad + proveedores.

No deberá considerarse que un establecimiento es tecnológicamente seguro simplemente por poseer equipos modernos.

La seguridad deberá medirse por su capacidad efectiva de resistir, detectar, responder y recuperarse ante incidentes.

45. Transparencia tecnológica

La información pública deberá permitir conocer, en términos generales:

- Cantidad de sistemas instalados
- Nivel de cobertura
- Inversión
- Disponibilidad
- Auditorías realizadas
- Incidentes agregados
- Acciones de mejora

No deberán divulgarse públicamente detalles técnicos que permitan identificar vulnerabilidades específicas.

46. Coordinación con las instituciones competentes

La protección tecnológica deberá coordinarse con las instituciones públicas que tengan competencias legales en:

- Telecomunicaciones
- Ciberseguridad
- Investigación criminal
- Protección de datos
- Administración pública
- Contratación
- Auditoría

RD Propone RD Propone

- Justicia

En materia de telecomunicaciones, la coordinación deberá respetar las competencias regulatorias correspondientes. La Ley 153-98 constituye el marco regulatorio básico de las telecomunicaciones en República Dominicana y establece las competencias de INDOTEL en la materia.

Cuando una situación tecnológica pueda constituir un delito de alta tecnología, deberán activarse los mecanismos previstos por la legislación correspondiente, incluyendo la Ley 53-07 cuando resulte aplicable.

47. Principio de continuidad institucional

La seguridad tecnológica deberá diseñarse para que ningún cambio de gobierno, ministro, director, proveedor, contratista, administración penitenciaria, provoque por sí mismo la pérdida de conocimiento, información o capacidad operacional.

La infraestructura crítica deberá pertenecer funcionalmente al Estado y mantenerse documentada.

48. Prohibición de sistemas opacos

Ningún sistema crítico deberá implementarse sin que el Estado conozca suficientemente:

- Qué función realiza
- Qué información procesa
- Dónde almacena información
- Quién puede acceder
- Cómo se audita
- Cómo se respalda
- Cómo se recupera
- Cómo se actualiza
- Cómo se desactiva
- Cómo se sustituye

La seguridad nacional no deberá utilizarse como justificación para permitir una dependencia tecnológica que impida al Estado conocer y controlar su propia infraestructura.

49. Principio de recuperación verificable

Ante una falla tecnológica grave, no bastará con restablecer aparentemente el servicio.

RD Propone RD Propone

Deberá verificarse:

- Integridad
- Funcionamiento
- Registros
- Configuraciones
- Controles
- Sincronización
- Disponibilidad
- Ausencia de modificaciones no autorizadas

La recuperación deberá ser documentada.

50. Principio rector del capítulo

El Sistema Nacional deberá asumir que:

La tecnología que protege la seguridad penitenciaria también debe ser protegida.

Por tanto, cámaras, sensores, sistemas de comunicación, controles de acceso, bases de datos, servidores, redes, sistemas de inteligencia y registros electrónicos deberán considerarse parte de la infraestructura crítica de seguridad.

El objetivo final será garantizar que el sistema pueda:

PREVENIR / DETECTAR / RESISTIR / RESPONDER / RECUPERAR / APRENDER.

La seguridad tecnológica penitenciaria deberá ser concebida, por tanto, como un sistema permanente de protección institucional y no como una simple adquisición de equipos.

CAPÍTULO XXII
RÉGIMEN DE ADQUISICIÓN, HOMOLOGACIÓN, CONTRATACIÓN Y CONTROL DE TECNOLOGÍAS Y PROVEEDORES DE SEGURIDAD PENITENCIARIA

1. Objeto

El presente capítulo establece los principios y mecanismos aplicables a la planificación, adquisición, evaluación, homologación, contratación, instalación, recepción, mantenimiento, actualización, sustitución y retiro de tecnologías destinadas a la seguridad penitenciaria.

Su finalidad será garantizar que las inversiones públicas destinadas al Sistema Nacional:

RD Propone RD Propone

1. Respondan a necesidades previamente identificadas
2. Sean técnicamente adecuadas
3. Puedan integrarse con la infraestructura existente
4. Sean sostenibles económicamente
5. Puedan ser auditadas
6. Reduzcan la dependencia tecnológica
7. Protejan la información estatal
8. Permitan continuidad operacional
9. Produzcan resultados verificables

2. Principio de necesidad previa

Ninguna adquisición tecnológica deberá iniciarse únicamente porque exista una tecnología disponible en el mercado. Antes de adquirir cualquier solución deberá determinarse:

- Cuál problema se pretende resolver
- Cuál es su magnitud
- Cuál es la situación actual
- Qué controles ya existen
- Qué deficiencias fueron identificadas
- Qué alternativas fueron consideradas
- Cuál resultado se espera
- Cómo se medirá dicho resultado

La regla será *primero identificar el problema; después diseñar la solución; finalmente adquirir la tecnología.*

3. Diagnóstico previo obligatorio

El diagnóstico deberá determinar, como mínimo:

- Infraestructura disponible
- Estado de los equipos
- Cobertura
- Vulnerabilidades
- Necesidades de personal
- Capacidad eléctrica
- Conectividad
- Capacidad de almacenamiento

RD Propone RD Propone

- Sistemas existentes
- Compatibilidad
- Necesidades de mantenimiento
- Riesgos
- Costo estimado de operación

El diagnóstico deberá evitar la duplicación innecesaria de sistemas.

4. Planificación plurianual

Las adquisiciones de infraestructura tecnológica crítica deberán formar parte de una planificación plurianual.

El Estado deberá considerar no solamente el costo de adquisición, sino también:

- Instalación
- Configuración
- Capacitación
- Licencias
- Mantenimiento
- Actualizaciones
- Reemplazo
- Soporte
- Energía
- Conectividad
- Almacenamiento
- Ciberseguridad
- Disposición final

La decisión deberá considerar el costo total de propiedad durante el ciclo de vida.

5. Integración con el Sistema Nacional

Ninguna tecnología crítica deberá adquirirse de manera aislada cuando su funcionamiento requiera integración con otros sistemas. Antes de aprobarse deberá determinarse su compatibilidad con:

- videovigilancia;
- control de acceso;
- sistemas de detección;
- monitoreo;

RD Propone RD Propone

- inteligencia;
- registro de incidentes;
- comunicaciones;
- infraestructura informática;
- sistemas de auditoría.

La tecnología deberá incorporarse a la arquitectura nacional y no convertirse en una plataforma independiente.

6. Interoperabilidad

Los sistemas deberán utilizar, cuando sea técnica y jurídicamente viable, estándares que permitan interoperabilidad.

Los pliegos técnicos deberán evitar especificaciones diseñadas innecesariamente para favorecer una marca determinada. Cuando una tecnología propietaria resulte necesaria por razones técnicas o de seguridad, deberá justificarse documentalmente.

7. Neutralidad tecnológica

Las especificaciones técnicas deberán describir preferentemente qué debe hacer el sistema, qué nivel de seguridad debe alcanzar, qué desempeño debe garantizar, cómo deberá integrarse, y cómo será verificado.

No deberán redactarse especificaciones cuyo único propósito sea reproducir las características comerciales de un producto específico, salvo justificación técnica suficiente.

8. Homologación de tecnologías críticas

El Sistema Nacional deberá establecer un mecanismo de homologación para tecnologías consideradas críticas. La homologación deberá evaluar, según corresponda:

- Seguridad
- Desempeño
- Compatibilidad
- Confiabilidad
- Interoperabilidad
- Ciberseguridad
- Capacidad de auditoría
- Mantenimiento

RD Propone RD Propone

- Disponibilidad de repuestos
- Soporte
- Vida útil
- Escalabilidad

La homologación no sustituirá el procedimiento legal de contratación pública. Su finalidad será determinar si una solución es técnicamente apta para ser considerada dentro del sistema.

9. Registro Nacional de Tecnologías Homologadas

Deberá establecerse un registro de soluciones tecnológicas que hayan sido evaluadas. El registro podrá contener:

- Fabricante
- Proveedor
- Categoría
- Versión
- Funciones
- Nivel de homologación
- Fecha
- Resultados de pruebas
- Limitaciones
- Compatibilidades
- Condiciones de mantenimiento
- Vigencia

La existencia de una tecnología en el registro no constituirá garantía absoluta de desempeño futuro.

10. Pruebas técnicas independientes

Las tecnologías críticas deberán ser sometidas a pruebas antes de su aceptación definitiva. Las pruebas deberán verificar, según corresponda:

- Funcionamiento
- Precisión
- Disponibilidad
- Integración
- Seguridad

RD Propone RD Propone

- Resistencia
- Almacenamiento
- Recuperación
- Trazabilidad
- Alarmas
- Capacidad de auditoría

Cuando la complejidad lo justifique, las pruebas deberán contar con participación de personal técnico independiente del proveedor.

11. Proyectos piloto

Cuando una tecnología no haya sido utilizada previamente por el Sistema Nacional, deberá considerarse la realización de un proyecto piloto. El piloto deberá establecer previamente:

- Objetivos
- Duración
- Indicadores
- Condiciones de prueba
- Riesgos
- Criterios de éxito
- Criterios de interrupción
- Mecanismo de evaluación

La decisión de expandir la tecnología deberá basarse en los resultados del piloto y no solamente en la demostración comercial del proveedor.

12. Prohibición de expansión automática

Antes de una expansión deberán evaluarse:

- Resultados
- Costos
- Mantenimiento
- Desempeño real
- Integración
- Capacitación
- Ciberseguridad
- Satisfacción operativa

RD Propone RD Propone

- Sostenibilidad presupuestaria

La expansión deberá responder a una decisión documentada.

13. Debida diligencia de proveedores

Los proveedores deberán someterse a los mecanismos de debida diligencia establecidos por el régimen de contratación pública y a los controles adicionales que resulten razonables por la criticidad del servicio. La evaluación podrá considerar:

- Existencia legal
- Experiencia
- Capacidad financiera
- Experiencia técnica
- Antecedentes contractuales
- Capacidad de soporte
- Conflictos de interés
- Estructura de propiedad cuando legalmente corresponda
- Cumplimiento tributario y laboral
- Antecedentes de incumplimiento
- Capacidad de continuidad

La contratación pública vigente ya incorpora mecanismos de debida diligencia, declaraciones de conflicto de interés y compromisos éticos de proveedores.

14. Integridad y anticorrupción

Los proveedores y contratistas deberán cumplir las normas de integridad aplicables a la contratación pública, deberán prevenirse especialmente:

- Colusión;
- Conflictos de interés;
- Sobornos;
- Especificaciones dirigidas;
- Manipulación de evaluaciones;
- Sobrevaloración;
- Pagos indebidos;
- Recepción irregular;
- Certificación falsa de cumplimiento.

RD Propone RD Propone

Cualquier indicio deberá ser remitido a las autoridades competentes conforme al procedimiento aplicable.

15. Separación de funciones

En los procesos de adquisición de tecnologías críticas deberán mantenerse separadas, cuando sea posible:

- Identificación de la necesidad
- Elaboración técnica
- Evaluación
- Contratación
- Recepción
- Certificación
- Pago
- Auditoría

Una misma persona no deberá controlar todo el ciclo de una adquisición crítica.

16. Comité Técnico de Evaluación

Para adquisiciones tecnológicas de especial importancia deberá constituirse un equipo técnico multidisciplinario. Podrá estar integrado, según la naturaleza del proyecto, por especialistas en:

- Seguridad penitenciaria
- Tecnología
- Telecomunicaciones
- Ciberseguridad
- Infraestructura
- Compras públicas
- Asuntos jurídicos
- Protección de datos
- Finanzas
- Operaciones

Los evaluadores deberán declarar posibles conflictos de interés.

17. Especificaciones técnicas orientadas a resultados

Las especificaciones deberán establecer indicadores objetivos. Por ejemplo:

RD Propone RD Propone

- Disponibilidad mínima
- Tiempo máximo de respuesta
- Capacidad
- Precisión
- Cobertura
- Tiempo de recuperación
- Interoperabilidad
- Seguridad
- Capacidad de almacenamiento
- Soporte

Deberá evitarse que la evaluación se reduzca a *"el equipo funciona"*. La pregunta deberá ser *"¿el sistema cumple el resultado de seguridad para el cual fue adquirido?"*

18. Pruebas de aceptación

La recepción definitiva de una tecnología crítica deberá producirse únicamente después de comprobar que cumple las condiciones contractuales. La prueba de aceptación deberá incluir:

1. Inspección física
2. Verificación de instalación
3. Pruebas funcionales
4. Pruebas de integración
5. Pruebas de seguridad
6. Revisión documental
7. Capacitación
8. Entrega de respaldos
9. Entrega de documentación técnica
10. Validación de garantías

19. Pagos vinculados al cumplimiento

Los contratos deberán estructurarse, cuando jurídicamente sea posible, de manera que los pagos y aceptaciones estén vinculados al cumplimiento verificable de las obligaciones.

No deberá pagarse como completamente ejecutado un proyecto cuya funcionalidad crítica todavía no haya sido demostrada.

20. Garantías de desempeño

RD Propone RD Propone

Los contratos de tecnologías críticas deberán establecer garantías adecuadas de desempeño. Podrán incluir:

- Disponibilidad
- Tiempos de respuesta
- Sustitución de equipos defectuosos
- Soporte técnico
- Reparación
- Actualización
- Recuperación
- Seguridad

El incumplimiento deberá producir las consecuencias contractuales correspondientes.

21. Acuerdos de nivel de servicio

Cuando se contraten servicios tecnológicos continuos deberán establecerse acuerdos de nivel de servicio. Estos deberán definir:

- Disponibilidad
- Tiempos de atención
- Tiempos de reparación
- Niveles de severidad
- Escalamiento
- Soporte
- Mantenimiento
- Reportes
- Consecuencias del incumplimiento

22. Mantenimiento obligatorio

El plan deberá establecer:

- Mantenimiento preventivo
- Mantenimiento correctivo
- Actualizaciones
- Sustitución de componentes
- Inventario de repuestos
- Responsables
- Frecuencia

RD Propone RD Propone

- Documentación

No deberá adquirirse infraestructura crítica sin determinar cómo será mantenida.

23. Repuestos y obsolescencia

Los contratos deberán prever mecanismos para enfrentar:

- Obsolescencia
- Discontinuación
- Falta de repuestos
- Finalización de soporte
- Incompatibilidad futura

Cuando un fabricante anuncie la finalización del soporte de un componente crítico, deberá realizarse una evaluación de riesgo.

24. Transferencia de conocimiento

Los proveedores deberán transferir al personal estatal los conocimientos necesarios para operar y mantener los sistemas. La transferencia podrá incluir:

- Capacitación
- Manuales
- Documentación
- Procedimientos
- Administración
- Diagnóstico
- Recuperación
- Mantenimiento básico

La finalidad será reducir progresivamente la dependencia operativa.

25. Documentación técnica

Todo proyecto deberá entregar documentación suficiente para permitir al Estado comprender y administrar la solución. Deberá incluir, según corresponda:

- Arquitectura
- Configuración
- Inventario
- Diagramas
- Procedimientos

RD Propone RD Propone

- Credenciales institucionales
- Licencias
- Garantías
- Mantenimiento
- Respaldo
- Recuperación

La documentación deberá permanecer bajo control institucional.

26. Control de acceso de proveedores

El acceso de personal externo a sistemas penitenciarios deberá cumplir los controles establecidos en el Capítulo XIX. El proveedor deberá poder ser identificado durante:

- ingreso;
- permanencia;
- intervención;
- acceso técnico;
- salida.

Toda intervención deberá quedar registrada.

27. Prohibición de acceso permanente no justificado

No deberá permitirse que un proveedor mantenga acceso permanente a sistemas críticos cuando dicho acceso ya no sea necesario. Los accesos deberán concederse por:

- Función
- Período
- Sistema
- Intervención autorizada

Al concluir el trabajo, deberán ser revocados o suspendidos.

28. Protección de la información entregada al proveedor

Deberán establecerse medidas sobre:

- Confidencialidad
- Almacenamiento
- Transferencia
- Copias
- Eliminación

RD Propone RD Propone

- Devolución
- Acceso de empleados del proveedor
- Subcontratistas

29. Subcontratación

La subcontratación de servicios críticos deberá ser conocida y autorizada conforme al contrato y al régimen aplicable. El contratista principal continuará siendo responsable frente al Estado por las obligaciones que le correspondan.

No deberá permitirse que una cadena indefinida de subcontrataciones elimine la capacidad estatal de identificar quién tiene acceso a su infraestructura.

30. Proveedores estratégicos

Cuando una empresa tenga participación relevante en infraestructura crítica, deberán evaluarse riesgos de dependencia. La institución deberá procurar que exista:

- Documentación
- Capacidad de sustitución
- Transferencia de conocimiento
- Alternativas técnicas
- Continuidad
- Control estatal de la información

31. Propiedad y control de la información

La información generada por sistemas penitenciarios deberá permanecer bajo control del Estado conforme al contrato y al ordenamiento jurídico aplicable.

El proveedor no deberá utilizarla para fines comerciales, entrenamiento de productos, publicidad u otros usos no autorizados. Cualquier tratamiento adicional deberá contar con fundamento jurídico y contractual suficiente.

32. Servicios en la nube

Cuando se utilicen servicios de computación en la nube para información penitenciaria, deberá evaluarse:

- Jurisdicción
- Ubicación
- Seguridad

RD Propone RD Propone

- Disponibilidad
- Respaldo
- Recuperación
- Acceso administrativo
- Cifrado
- Continuidad
- Migración

Los servicios críticos deberán contar con mecanismos que permitan recuperar la información y trasladarla a otra plataforma cuando sea necesario.

33. Código, configuraciones y activos digitales

Cuando resulte jurídicamente y técnicamente procedente, los contratos deberán establecer mecanismos para garantizar que el Estado conserve acceso suficiente a:

- Configuraciones
- Documentación
- Interfaces
- Integraciones
- Claves institucionales
- Certificados
- Bases de datos

Cuando la adquisición incluya desarrollo específico para el Estado, deberán establecerse contractualmente los derechos correspondientes sobre el producto desarrollado.

34. Control de licencias

Las licencias de software crítico deberán ser inventariadas. El Estado deberá conocer:

- Cantidad
- Duración
- Costo
- Fecha de renovación
- Dependencia
- Consecuencias de vencimiento

No deberá permitirse que la expiración inesperada de una licencia provoque la interrupción de una función crítica de seguridad.

RD Propone RD Propone

35. Costos recurrentes

Antes de adquirir una solución deberán calcularse los costos recurrentes. Estos podrán incluir:

- Licencias
- Conectividad
- Almacenamiento
- Mantenimiento
- Soporte
- Actualizaciones
- Repuestos
- Capacitación
- Energía

Una solución aparentemente económica que genere costos recurrentes desproporcionados deberá ser evaluada bajo su costo total de propiedad.

36. Evaluación de alternativas

Para proyectos de importancia nacional deberá documentarse por qué se seleccionó determinada solución. La evaluación deberá considerar:

- Alternativa existente
- Alternativa tecnológica
- Alternativa institucional
- Costo
- Desempeño
- Riesgo
- Mantenimiento
- Escalabilidad
- Interoperabilidad

El objetivo no será seleccionar necesariamente la tecnología más sofisticada, sino aquella que pueda cumplir de forma verificable la necesidad identificada dentro de las condiciones institucionales existentes.

37. Prohibición de compras fragmentadas

RD Propone RD Propone

No deberán dividirse artificialmente adquisiciones relacionadas con una misma solución con el propósito de alterar el procedimiento de contratación aplicable. Los proyectos deberán planificarse considerando su verdadera dimensión.

38. Compras de emergencia

Cuando ocurra una situación que requiera una adquisición urgente, deberán aplicarse los mecanismos excepcionales establecidos por la legislación de contratación pública. La urgencia no deberá convertirse en una autorización general para:

- Eliminar controles
- Omitir documentación
- Favorecer proveedores
- Adquirir tecnologías no probadas
- Evitar auditorías

Toda contratación excepcional deberá quedar debidamente documentada.

39. Contrataciones vinculadas a seguridad nacional

Cuando una contratación pueda estar sujeta a un régimen excepcional por razones legalmente reconocidas de seguridad o defensa, deberán cumplirse estrictamente las condiciones establecidas por el ordenamiento jurídico.

La clasificación de una adquisición como relacionada con seguridad penitenciaria no deberá utilizarse automáticamente para excluirla de los controles ordinarios. La excepción deberá ser:

legal, necesaria, documentada y proporcional.

40. Auditoría de proveedores

Los proveedores de tecnologías críticas podrán ser sometidos a auditorías relacionadas con:

- Cumplimiento contractual
- Seguridad
- Acceso a información
- Mantenimiento
- Desempeño
- Facturación

RD Propone RD Propone

- Inventario
- Continuidad
- Subcontratación

La auditoría deberá respetar los derechos y obligaciones contractuales correspondientes.

41. Evaluación posterior a la contratación

Después de la implementación deberá evaluarse si el proyecto alcanzó sus objetivos. La evaluación deberá comparar:

Objetivo inicial / Resultado obtenido / Costo real / Problemas encontrados / Beneficios / Correcciones necesarias

Esta evaluación deberá alimentar futuras decisiones de adquisición.

42. Registro de desempeño de proveedores

El Sistema Nacional deberá mantener información institucional sobre el desempeño contractual de proveedores, conforme al régimen jurídico aplicable. Podrá registrarse:

- Cumplimiento
- Retrasos
- Fallas
- Disponibilidad
- Calidad
- Atención
- Cumplimiento de seguridad
- Mantenimiento
- Incidentes
- Acciones correctivas

El registro deberá utilizarse para fortalecer la planificación y gestión contractual conforme a la normativa vigente.

43. Proveedores y conflictos de interés

Los funcionarios que participen en procesos de adquisición deberán declarar los conflictos de interés que correspondan. No deberán participar en evaluaciones quienes tengan intereses personales, familiares, comerciales o económicos incompatibles con la imparcialidad exigida.

44. Canal de denuncias

RD Propone RD Propone

Deberá existir un mecanismo seguro para reportar:

- Manipulación de especificaciones
- Favoritismo
- Colusión
- Soborno
- Conflictos de interés
- Sobrevaloración
- Recepción irregular
- Falsificación
- Incumplimiento tecnológico

Las denuncias deberán ser evaluadas por las autoridades competentes.

45. Prohibición de aceptación informal

Ningún equipo o sistema crítico deberá considerarse recibido únicamente porque haya sido instalado. La aceptación deberá sustentarse en documentación y pruebas.

Deberá existir una diferencia clara entre:

Instalado - Probado - Aceptado - Puesto en producción

46. Retiro y sustitución

Cuando una tecnología llegue al final de su vida útil o deje de cumplir los requisitos de seguridad, deberá existir un procedimiento de sustitución. El retiro deberá contemplar:

- Protección de información
- Eliminación segura de datos
- Recuperación de activos
- Disposición ambiental cuando corresponda
- Actualización del inventario
- Sustitución
- Documentación

47. Evaluación de impacto antes de tecnologías de alta sensibilidad

Antes de implementar tecnologías capaces de producir un impacto significativo sobre derechos fundamentales, deberá realizarse una evaluación jurídica, técnica y operativa. Deberá determinarse:

RD Propone RD Propone

- Finalidad
- Necesidad
- Proporcionalidad
- Riesgos
- Controles
- Responsables
- Mecanismos de supervisión
- Mecanismos de revisión

La sofisticación tecnológica no sustituirá la justificación jurídica.

48. Prohibición de tecnologías dañinas

No deberán adquirirse ni implementarse tecnologías cuyo funcionamiento implique daños indiscriminados o riesgos innecesarios para personas, infraestructura, sistemas médicos, sistemas de emergencia, comunicaciones institucionales y equipos esenciales.

Las tecnologías deberán orientarse a *prevenir, detectar, controlar y responder,* no a causar daños como mecanismo principal de seguridad.

49. Banco Nacional de soluciones y experiencias

El Sistema Nacional deberá mantener un registro de:

- Tecnologías evaluadas
- Pilotos realizados
- Resultados
- Fallas
- Costos
- Experiencias de implementación
- Soluciones descartadas
- Razones de descarte

Esto permitirá evitar repetir adquisiciones fallidas y facilitar la planificación futura.

50. Principio de eficiencia pública

El objetivo del régimen de adquisición no será gastar más en tecnología. Será obtener *mayor seguridad efectiva por cada peso invertido.* Por ello deberán priorizarse soluciones que:

- Resuelvan problemas concretos

RD Propone RD Propone

- Puedan mantenerse
- Sean interoperables
- Sean auditables
- Tengan costos sostenibles
- Puedan escalarse
- Reduzcan vulnerabilidades
- Produzcan resultados medibles

51. Indicadores de contratación tecnológica

El Sistema Nacional deberá medir, entre otros:

- Porcentaje de proyectos entregados a tiempo
- Porcentaje de proyectos dentro del presupuesto
- Porcentaje de sistemas que superan pruebas de aceptación
- Disponibilidad de sistemas
- Costo de mantenimiento;
- Cantidad de fallas
- Tiempo de reparación
- Dependencia de proveedores
- Porcentaje de contratos con acuerdos de nivel de servicio
- Porcentaje de tecnologías homologadas
- Porcentaje de proyectos sometidos a evaluación posterior

52. Evaluación anual del mercado tecnológico

El Estado deberá revisar periódicamente la evolución de las tecnologías disponibles. La revisión deberá identificar:

- Nuevas soluciones
- Cambios de costos
- Nuevas vulnerabilidades
- Tecnologías obsoletas
- Alternativas nacionales
- Posibilidades de interoperabilidad
- Oportunidades de innovación

Esta evaluación no deberá convertirse en una obligación de comprar nuevas tecnologías.

RD Propone RD Propone

53. Participación de capacidades nacionales

Cuando exista capacidad técnica nacional suficiente y competitiva, deberán evaluarse las posibilidades de participación de empresas, universidades, centros tecnológicos y profesionales dominicanos, siempre dentro del marco de contratación pública y sin sacrificar los requisitos de seguridad.

Podrán priorizarse, cuando la legislación lo permita y existan condiciones objetivas, proyectos de:

- Desarrollo
- Mantenimiento
- Integración
- Análisis
- Capacitación
- Investigación

54. Innovación controlada

Toda innovación deberá cumplir:

Problema definido - hipótesis - piloto - medición - evaluación - decisión

No deberá incorporarse una tecnología únicamente por ser novedosa.

55. Principio de no dependencia

El Estado deberá conservar capacidad suficiente para operar y recuperar sus sistemas críticos aun cuando un proveedor:

- Quiebre
- Abandone el mercado
- Termine el contrato
- Deje de prestar soporte
- Aumente significativamente sus costos
- Pierda capacidad técnica

La continuidad institucional no deberá depender de la voluntad de una empresa.

56. Responsabilidad por incumplimiento

RD Propone RD Propone

Los incumplimientos contractuales deberán generar las consecuencias establecidas en el contrato y en la legislación aplicable.

Cuando existan indicios de fraude, corrupción, falsificación, sabotaje u otra conducta ilícita, deberán remitirse a las autoridades correspondientes.

57. Integración con la política presupuestaria

Las adquisiciones deberán estar vinculadas con la planificación presupuestaria nacional. El Estado deberá evitar comprar equipos sin presupuesto de mantenimiento. Todo proyecto tecnológico crítico deberá identificar desde su planificación:

- Inversión inicial
- Gasto recurrente
- Mantenimiento
- Actualización
- Reemplazo
- Capacitación

58. Evaluación de costo-beneficio

Los proyectos de gran impacto deberán incluir una evaluación que permita determinar:

- Inversión
- Costos recurrentes
- Reducción esperada del riesgo
- Beneficios operativos
- Alternativas
- Riesgos residuales

El análisis deberá evitar presentar como ahorro una solución que simplemente traslade el costo hacia años posteriores.

59. Revisión periódica del régimen

El presente régimen deberá revisarse periódicamente para incorporar:

- Cambios legales
- Cambios tecnológicos
- Nuevas amenazas
- Experiencias de implementación

RD Propone RD Propone

- Resultados de auditorías
- Recomendaciones técnicas

La revisión deberá mantener el principio fundamental:

tecnología al servicio de la seguridad, no seguridad subordinada al proveedor tecnológico.

CAPÍTULO XXIII
RÉGIMEN NACIONAL DE CAPACITACIÓN, CERTIFICACIÓN Y PROFESIONALIZACIÓN DEL PERSONAL DE SEGURIDAD PENITENCIARIA

1. Objeto

El presente capítulo establece las bases para la capacitación, certificación, actualización y evaluación permanente del personal que participe directa o indirectamente en la seguridad penitenciaria. Su finalidad será asegurar que las personas responsables de custodiar, supervisar, operar, mantener, administrar, auditar, investigar y analizar los sistemas de seguridad penitenciaria posean las competencias necesarias para desempeñar sus funciones.

La profesionalización será considerada un componente de seguridad y no únicamente una política de recursos humanos.

2. Principio de competencia profesional

Ninguna función crítica deberá asignarse exclusivamente por antigüedad, disponibilidad o designación administrativa. La persona asignada deberá demostrar las competencias necesarias para la función.

La institución deberá distinguir entre:

tener un cargo y estar certificado para ejercer una función crítica específica.

3. Clasificación de funciones

El Sistema Nacional deberá identificar, como mínimo, las siguientes áreas funcionales:

1. Seguridad y custodia
2. Control de acceso
3. Monitoreo y videovigilancia
4. Operación de sistemas tecnológicos
5. Telecomunicaciones

RD Propone RD Propone

6. Ciberseguridad
7. Inteligencia y análisis
8. Preservación de evidencia
9. Investigación administrativa
10. Mantenimiento tecnológico
11. Gestión de incidentes
12. Supervisión
13. Auditoría
14. Administración de sistemas
15. Gestión de proveedores

Cada función deberá contar con requisitos específicos.

4. Perfiles de competencia

Para cada función crítica deberá establecerse un perfil que determine:

- Conocimientos mínimos
- Habilidades
- Experiencia
- Formación
- Certificaciones
- Responsabilidades
- Restricciones
- Capacitación periódica

El perfil deberá actualizarse conforme evolucionen las amenazas y tecnologías.

5. Formación inicial

Ninguna persona deberá asumir por primera vez una función crítica sin recibir la formación correspondiente. La formación inicial deberá incluir, según el cargo:

- Seguridad penitenciaria
- Derechos fundamentales
- Legislación aplicable
- Protocolos institucionales
- Uso de tecnología
- Protección de información

RD Propone RD Propone

- Manejo de incidentes
- Preservación de evidencia
- Etica pública
- Prevención de corrupción
- Comunicación institucional
- Primeros auxilios
- Gestión de situaciones críticas

6. Formación específica según función

La capacitación deberá diferenciarse. Un operador de cámaras no necesita exactamente la misma formación que:

- Un administrador de servidores
- Un investigador
- Un técnico de telecomunicaciones
- Un custodio
- Un auditor
- Un analista de inteligencia

La especialización deberá evitar la formación genérica como único requisito.

7. Certificación de funciones críticas

La certificación deberá acreditar que la persona:

- Conoce el sistema
- Conoce los protocolos
- Comprende sus límites
- Puede responder ante incidentes
- Conoce sus responsabilidades
- Puede proteger evidencia
- Conoce las reglas de acceso a información;
- Comprende las consecuencias de incumplir.

8. Vigencia de la certificación

Las certificaciones deberán tener vigencia limitada. Su renovación deberá requerir:

- Actualización
- Evaluación

RD Propone RD Propone

- Capacitación
- Revisión de competencias

La certificación no deberá convertirse en un reconocimiento permanente independiente del desempeño.

9. Recertificación

Podrá requerirse una evaluación extraordinaria cuando:

- Cambie sustancialmente la tecnología
- Se modifique el procedimiento
- Ocurra un incidente grave
- Se detecten deficiencias
- La persona deje de ejercer la función durante un período prolongado

10. Evaluación teórica y práctica

La certificación deberá combinar:

conocimiento teórico + desempeño práctico.

La persona deberá demostrar que puede actuar correctamente ante escenarios controlados. Las evaluaciones podrán incluir:

- Pruebas escritas
- Ejercicios
- Simulaciones
- Resolución de incidentes
- Análisis de casos
- Prácticas supervisadas

11. Simulaciones de incidentes

El Sistema Nacional deberá desarrollar ejercicios periódicos para comprobar la capacidad de respuesta. Podrán simularse, de manera controlada:

- Detección de dispositivos
- Pérdida de cámaras
- Alteración de sistemas
- Fallas de comunicación
- Incidentes cibernéticos

RD Propone RD Propone

- Pérdida de energía
- Intento de manipulación de registros
- Hallazgo de evidencia
- Incidentes con terceros

Los ejercicios no deberán divulgar públicamente vulnerabilidades específicas de los establecimientos.

12. Formación en derechos fundamentales

Todo el personal deberá conocer los límites jurídicos de su actuación. La capacitación deberá incluir:

- Dignidad humana
- Debido proceso
- Privacidad
- Protección de datos
- Comunicaciones legítimas
- Reglas de inspección
- Tratamiento de personas privadas de libertad
- Actuación proporcional
- Prohibición de discriminación
- Uso adecuado de la autoridad

La seguridad no deberá utilizarse como justificación para actuaciones arbitrarias.

13. Formación en evidencia digital

El personal que pueda participar en la detección o preservación de dispositivos electrónicos deberá conocer la diferencia entre:

encontrar - asegurar - preservar - documentar - analizar

La formación deberá dejar claro que:

incautar un dispositivo no equivale a estar autorizado para explorar su contenido.

14. Formación en cadena de custodia

El personal deberá aprender:

- Identificación

RD Propone RD Propone

- Documentación
- Embalaje
- Almacenamiento
- Traslado
- Recepción
- Entrega
- Registro

Los errores de cadena de custodia deberán ser considerados una deficiencia grave cuando comprometan la integridad de una evidencia.

15. Formación en ciberseguridad

El personal con acceso a sistemas tecnológicos deberá recibir capacitación en:

- Credenciales
- Autenticación
- Phishing
- Ingeniería social
- Malware
- Dispositivos externos
- Protección de información
- Accesos no autorizados
- Reporte de incidentes

La capacitación deberá adaptarse al nivel de acceso de cada persona.

16. Formación en inteligencia y análisis

El personal dedicado a inteligencia deberá recibir formación en:

- Análisis de información
- Evaluación de fuentes
- Identificación de patrones
- Elaboración de hipótesis
- Análisis de vínculos
- Protección de fuentes
- Tratamiento de información sensible
- Separación entre indicio, inteligencia y evidencia

RD Propone RD Propone

17. Formación contra sesgos y errores de interpretación

Los analistas deberán conocer los riesgos de:

- Conclusiones prematuras
- Confirmación de hipótesis
- Interpretación incorrecta de patrones
- Correlaciones falsas
- Exceso de confianza en sistemas automatizados

La información deberá analizarse con criterios verificables.

18. Formación en inteligencia artificial

Cuando se utilicen herramientas de inteligencia artificial, los operadores deberán conocer:

- Capacidades
- Limitaciones
- Posibles errores
- Falsos positivos
- Falsos negativos
- Manipulación
- Necesidad de verificación humana

La herramienta deberá apoyar al funcionario, no sustituir su responsabilidad.

19. Formación en tecnología de detección

El personal responsable de sistemas de detección deberá comprender:

- Funcionamiento general
- Condiciones normales
- Fuentes de falsas alarmas
- Mantenimiento
- Reporte de fallas
- Procedimientos ante alertas

20. Formación de operadores de videovigilancia

Los operadores deberán estar capacitados para:

RD Propone RD Propone

- Monitorear
- Identificar anomalías
- Documentar incidentes
- Proteger información
- Preservar grabaciones
- Responder ante pérdida de señal
- Escalar incidentes

Deberán conocer las limitaciones de las cámaras y evitar interpretar una imagen fuera de contexto.

21. Formación del personal técnico

Los técnicos deberán conocer:

- Mantenimiento
- Ciberseguridad
- Control de acceso
- Documentación
- Gestión de cambios
- Respaldo
- Recuperación
- Protección de información

Las intervenciones técnicas deberán quedar registradas.

22. Formación del personal de mando

Los responsables de establecimientos y supervisores deberán recibir formación adicional en:

- Gestión de incidentes
- Toma de decisiones
- Coordinación interinstitucional
- Preservación de evidencia
- Continuidad operacional
- Gestión de riesgos
- Supervisión de personal
- Control de proveedores

RD Propone RD Propone

El mando deberá comprender el funcionamiento general del sistema aunque no sea especialista técnico.

23. Formación sobre corrupción y complicidad

El programa deberá incluir mecanismos para identificar y prevenir:

- Sobornos
- Favores
- Introducción de objetos
- Ocultamiento
- Manipulación de registros
- Uso indebido de credenciales
- Colaboración con terceros
- Conflictos de interés

La capacitación deberá explicar las consecuencias administrativas, disciplinarias y penales que correspondan.

24. Deber de reporte

El personal deberá conocer su obligación de reportar:

- Incidentes
- Vulnerabilidades
- Fallas
- Accesos indebidos
- Intentos de corrupción
- Pérdida de equipos
- Manipulación de sistemas
- Alteración de registros

El silencio deliberado ante un hecho relevante deberá ser investigado conforme a las circunstancias.

25. Protección al denunciante de buena fe

El sistema deberá establecer mecanismos para proteger a quienes reporten de buena fe:

- Corrupción
- Manipulación

RD Propone RD Propone

- Fallas críticas
- Vulnerabilidades
- Amenazas
- Incumplimientos

La protección deberá respetar los procedimientos legales y evitar represalias indebidas.

26. Evaluación de desempeño

Deberán analizarse:

- Cumplimiento de protocolos
- Calidad de reportes
- Respuesta ante incidentes
- Errores
- Formación
- Cumplimiento de controles
- Comportamiento ético
- Observaciones de auditoría

La evaluación deberá realizarse con criterios objetivos.

27. Errores, negligencia y conducta deliberada

El sistema deberá distinguir claramente entre error humano no intencional, negligencia, incumplimiento reiterado, omisión deliberada, conducta intencionalmente dañina. No toda falla deberá recibir la misma consecuencia. La respuesta deberá guardar proporción con la conducta y sus efectos.

28. Suspensión de certificación

La certificación podrá ser suspendida preventivamente cuando existan circunstancias objetivas que hagan necesario retirar temporalmente a una persona de una función crítica, conforme al procedimiento aplicable.

La medida deberá ser revisable. No deberá convertirse en una sanción anticipada.

29. Revocación de certificación

La certificación podrá ser revocada cuando, mediante el procedimiento correspondiente, se determine que la persona:

RD Propone RD Propone

- Incumplió gravemente sus obligaciones
- Manipuló deliberadamente sistemas
- Comprometió evidencia
- Utilizó indebidamente información
- Permitió accesos no autorizados
- Actuó de manera incompatible con la función certificada

La revocación deberá estar debidamente motivada.

30. Registro Nacional de Certificaciones

El Sistema Nacional deberá mantener un registro actualizado de las certificaciones correspondientes a funciones críticas, este, deberá permitir conocer:

- Persona certificada
- Función
- Nivel
- Fecha de certificación
- Fecha de vencimiento
- Recertificaciones
- Suspensiones
- Revocaciones

El acceso al registro deberá estar restringido según corresponda.

31. Prohibición de asignación sin certificación

Las funciones críticas no deberán ser ejercidas permanentemente por personal que no cumpla los requisitos de certificación establecidos.

Cuando exista una situación excepcional, deberá existir autorización temporal y supervisión adecuada.

32. Capacitación de emergencia

El personal deberá recibir formación específica antes de implementar nuevas tecnologías o procedimientos críticos. No deberá ocurrir:

Instalación - puesta en servicio - capacitación después

La secuencia deberá ser:

RD Propone RD Propone

33. Formación continua

La formación deberá adaptarse a:

- Nuevos riesgos
- Nuevos sistemas
- Incidentes recientes
- Cambios legislativos
- Resultados de auditorías
- Nuevas tecnologías

34. Banco de conocimientos

El Sistema Nacional deberá mantener materiales institucionales sobre:

- Procedimientos
- Incidentes
- Lecciones aprendidas
- Errores frecuentes
- Buenas prácticas
- Cambios tecnológicos
- Modificaciones legales

El conocimiento generado por un establecimiento deberá poder beneficiar a los demás.

35. Formación interinstitucional

Cuando un incidente requiera coordinación entre varias instituciones, podrán desarrollarse programas conjuntos de capacitación. Podrán participar, según sus competencias:

- Ministerio de Justicia
- Dirección General de Servicios Penitenciarios y Correccionales
- Ministerio Público
- INDOTEL
- Instituciones de Seguridad
- Organos de control
- Poder Judicial, dentro de sus competencias
- Universidades y centros especializados

RD Propone RD Propone

36. Formación especializada avanzada

Deberán establecerse programas especializados para:

- Ciberseguridad
- Análisis de inteligencia
- Evidencia digital
- Administración de sistemas
- Telecomunicaciones
- Análisis de datos
- Auditoría tecnológica
- Investigación de incidentes

El Estado deberá procurar desarrollar capacidades internas para reducir la dependencia permanente de consultores externos.

37. Cooperación académica

El Estado podrá establecer acuerdos con:

- Universidades
- Institutos técnicos
- Centros de investigación
- Organizaciones especializadas

Los acuerdos podrán incluir:

- Formación
- Investigación
- Simulaciones
- Desarrollo tecnológico
- Evaluación
- Certificaciones

Toda cooperación deberá respetar las reglas de seguridad y protección de información.

38. Certificación de instructores

Los instructores responsables de formar al personal en funciones críticas deberán acreditar las competencias necesarias. Deberán mantenerse actualizados.

39. Evaluación de calidad de la capacitación

RD Propone RD Propone

No deberá medirse la capacitación únicamente por cantidad de personas capacitadas. También deberá medirse:

- Aprobación
- Desempeño práctico
- Reducción de errores
- Capacidad de respuesta
- Resultados de simulaciones
- Incidentes asociados a errores
- Actualización

La capacitación deberá medirse por resultados.

40. Simulaciones nacionales

Periódicamente deberán realizarse ejercicios coordinados que permitan comprobar la capacidad del sistema completo. Por ejemplo:

Detección - alerta - validación - intervención - preservación - investigación - comunicación interinstitucional - cierre

41. Evaluación posterior a incidentes

Cuando un incidente relevante revele una deficiencia de capacitación, deberá establecerse:

- Qué conocimiento faltó
- Quiénes necesitaban esa capacitación
- Qué contenido debe modificarse
- Cuándo deberá impartirse
- Cómo se verificará la mejora

42. Formación de proveedores y contratistas

Los proveedores que tengan acceso a establecimientos o sistemas críticos deberán recibir la orientación necesaria sobre:

- Seguridad
- Acceso
- Confidencialidad
- Protección de información

RD Propone RD Propone

- Reporte de incidentes
- Uso de equipos
- Zonas restringidas

La capacitación del proveedor no sustituirá sus obligaciones contractuales.

43. Evaluación de personal técnico externo

Cuando un proveedor asigne personal técnico a infraestructura crítica, el Estado deberá verificar que dicho personal cumpla los requisitos establecidos. Deberá mantenerse trazabilidad de:

- Identidad
- Autorización
- Función
- Período
- Sistema intervenido

44. Profesionalización de la carrera penitenciaria

El Estado deberá procurar que la formación y certificación se integren progresivamente a un modelo profesional de carrera. La adquisición de nuevas competencias deberá poder reflejarse en:

- Especialización
- Responsabilidades
- Desarrollo profesional
- Oportunidades de promoción conforme al régimen aplicable

La profesionalización deberá incentivar la permanencia de personal competente.

45. Principio de mérito y competencia

Las funciones técnicas y de seguridad deberán asignarse conforme a criterios objetivos de:

- Preparación
- Experiencia
- Desempeño
- Certificación
- Integridad

RD Propone RD Propone

- Competencias

La designación para una función crítica deberá poder justificarse documentalmente.

46. Rotación controlada

En funciones especialmente sensibles deberá evaluarse la rotación periódica cuando resulte conveniente para reducir:

- Dependencia excesiva de una persona
- Concentración de conocimiento
- Riesgos de corrupción
- Conflictos de interés

La rotación deberá preservar la continuidad operacional.

47. Separación de funciones

Cuando una función implique riesgo significativo, deberá evitarse que una sola persona pueda *Autorizar, ejecutar, modificar, borrar, auditar* la misma operación sin controles independientes. La separación deberá diseñarse de acuerdo con el nivel de riesgo.

48. Control de acceso después del traslado

Cuando una persona sea trasladada a otra función deberá revisarse inmediatamente:

- Certificación
- Permisos
- Accesos
- Credenciales
- Equipos asignados

No deberá mantenerse automáticamente un nivel de acceso correspondiente a su puesto anterior.

49. Evaluación de fatiga y condiciones de trabajo

La administración deberá procurar condiciones organizativas que reduzcan errores derivados de:

- Jornadas excesivas
- Falta de descansos
- Sobrecarga

RD Propone RD Propone

- Turnos inadecuados
- Insuficiencia de personal

El objetivo será reducir riesgos operativos y proteger tanto al personal como a las personas bajo custodia.

50. Principio de responsabilidad profesional

El personal que opere sistemas críticos deberá comprender que su actuación forma parte de una cadena de seguridad. Una omisión aparentemente pequeña puede afectar:

Detección - respuesta - evidencia - investigación - seguridad

Por ello, cada función deberá estar acompañada de responsabilidades claramente definidas.

51. Indicadores de profesionalización

El Sistema Nacional deberá medir, entre otros:

- Porcentaje de personal certificado
- Porcentaje de certificaciones vigentes
- Horas de capacitación
- Resultados de evaluaciones
- Desempeño en simulaciones
- Incidentes asociados a errores
- Porcentaje de personal técnico actualizado
- Tiempo requerido para certificar nuevos funcionarios
- Porcentaje de proveedores capacitados
- Cumplimiento de recertificación

52. Auditoría del sistema de capacitación

El sistema de capacitación deberá ser auditado periódicamente, pudiendo determinar:

- Si los contenidos son adecuados
- Si las certificaciones son válidas
- Si las evaluaciones son objetivas
- Si la formación produce resultados
- Si existen brechas
- Si los recursos se utilizan correctamente

RD Propone RD Propone

53. Revisión curricular

Los contenidos deberán revisarse periódicamente para incorporar:

- Nuevas tecnologías
- Nuevas amenazas
- Nuevas modalidades delictivas
- Nuevas normas
- Lecciones aprendidas
- Resultados de auditorías

54. Principio de aprendizaje institucional

Cada incidente relevante deberá responder también una pregunta:

¿qué debemos enseñar mejor?

Cuando un incidente revele una deficiencia humana, el Estado deberá determinar si se trata de:

- Falta de conocimiento
- Falta de práctica
- Falta de supervisión
- Falta de recursos
- Procedimiento incorrecto
- Incumplimiento deliberado

La solución deberá corresponder a la causa.

55. Prohibición de utilizar la capacitación como sustituto de controles

La capacitación es necesaria, pero no deberá utilizarse como sustituto de:

- Tecnología adecuada
- Supervisión
- Procedimientos
- Auditoría
- Infraestructura
- Controles de acceso

El sistema deberá asumir que *las personas pueden equivocarse*, por lo que los controles deberán diseñarse para detectar y limitar esos errores.

RD Propone RD Propone

56. Principio de defensa en profundidad humana

La seguridad deberá construirse mediante varias capas:

personal capacitado + procedimientos claros + tecnología + supervisión + auditoría + investigación.

Ninguna persona deberá ser considerada la única barrera entre el sistema y una vulnerabilidad.

57. Formación ética

Todo programa deberá incorporar principios de:

- Integridad
- Servicio público
- Confidencialidad
- Respeto
- Responsabilidad
- Imparcialidad
- Rechazo a la corrupción

La ética deberá considerarse una competencia profesional.

58. Régimen de actualización tecnológica

Cada vez que se incorpore una nueva tecnología crítica deberá evaluarse si:

- Los perfiles existentes siguen siendo adecuados
- Se requiere nueva certificación
- Debe modificarse el currículo
- Deben actualizarse los procedimientos

La tecnología no deberá ponerse en funcionamiento antes de preparar al personal que tendrá que operarla.

59. Evaluación nacional de madurez profesional

Periódicamente deberá evaluarse el nivel de profesionalización de cada establecimiento. La evaluación podrá considerar:

personal + certificaciones + capacitación + desempeño + supervisión + incidentes + auditorías.

Los resultados deberán utilizarse para priorizar recursos y capacitación.

RD Propone RD Propone

CAPÍTULO XXIV
SISTEMA NACIONAL DE CONTROL DE ACCESO, MOVILIDAD INTERNA Y TRAZABILIDAD DE PERSONAS, VEHÍCULOS, BIENES Y EQUIPOS

1. Objeto

El presente capítulo establece el Sistema Nacional de Control de Acceso, Movilidad Interna y Trazabilidad de Personas, Vehículos, Bienes y Equipos dentro de los establecimientos penitenciarios y demás instalaciones vinculadas al Sistema Penitenciario y Correccional.

Su finalidad será impedir, detectar y documentar accesos no autorizados, movimientos irregulares, introducción de objetos prohibidos, utilización indebida de credenciales, circulación no autorizada de equipos y cualquier otra circunstancia que pueda comprometer la seguridad del establecimiento, la integridad de las personas o la administración penitenciaria.

El sistema deberá permitir conocer, dentro de los límites establecidos por la Constitución y las leyes:

quién ingresó, cuándo ingresó, con qué autorización, a qué área podía acceder, qué bienes o equipos introdujo, por dónde se desplazó cuando corresponda, cuándo salió y qué incidencias fueron registradas durante su permanencia.

2. Principios rectores

El Sistema se regirá por los siguientes principios:

a) Legalidad
b) Necesidad
c) Proporcionalidad
d) Respeto a la dignidad humana
e) Igualdad y no discriminación
f) Mínima intervención necesaria
g) Trazabilidad
h) Responsabilidad individual
i) Separación de funciones
j) Integridad de los registros
k) Protección de datos personales

RD Propone RD Propone

l) Seguridad de la información
m) Supervisión humana
n) Rendición de cuentas
o) Auditabilidad
p) Continuidad operacional
q) Presunción de regularidad mientras no exista evidencia suficiente en contrario

Ningún sistema automatizado podrá sustituir las garantías jurídicas aplicables a las personas.

3. Clasificación de las áreas penitenciarias

Cada establecimiento deberá contar con una clasificación de sus espacios según nivel de riesgo y función. Como mínimo podrán establecerse:

Nivel I	Áreas administrativas y de acceso general controlado.
Nivel II	Áreas operativas y de servicios.
Nivel III	Áreas de circulación restringida.
Nivel IV	Áreas críticas de seguridad.
Nivel V	Áreas de máxima restricción, cuando las características del establecimiento lo justifiquen.

La clasificación deberá considerar, entre otros elementos:

- Presencia de personas privadas de libertad
- Manejo de información sensible
- Infraestructura tecnológica
- Sistemas de comunicación
- Depósitos
- Areas médicas
- Salas de servidores
- Centros de monitoreo
- Areas de evidencias
- Arsenales o depósitos de seguridad
- Accesos perimetrales
- Talleres
- Zonas de mantenimiento

RD Propone RD Propone

- Areas de recepción y despacho de bienes

La clasificación será revisada periódicamente y después de incidentes relevantes.

4. Principio de acceso mínimo necesario

Ninguna persona deberá tener acceso a una zona determinada simplemente por pertenecer a una institución, empresa o categoría profesional. El acceso deberá corresponder:

1. A la función que desempeña;
2. A la tarea autorizada;
3. Al tiempo necesario;
4. Al área necesaria;
5. Al nivel de riesgo correspondiente.

La autorización de acceso deberá poder ser modificada, suspendida o cancelada cuando cambien las funciones, exista una investigación, se produzca una pérdida de credencial o desaparezca la causa que justificaba el acceso.

5. Identificación individual

Toda persona que ingrese a un establecimiento penitenciario deberá encontrarse debidamente identificada. El sistema podrá utilizar, según la categoría de usuario y las condiciones legales y técnicas:

- Documento oficial de identidad
- Credenciales institucionales
- Tarjetas electrónicas
- Códigos personales
- Sistemas biométricos
- Autenticación multifactor
- Mecanismos temporales para visitantes
- Otros mecanismos tecnológicos homologados

La utilización de mecanismos biométricos deberá estar sustentada en una finalidad legítima, ser proporcional al riesgo y cumplir las normas aplicables sobre protección de datos personales.

RD Propone RD Propone

6. Credenciales institucionales

Cada credencial deberá estar vinculada a una persona determinada por lo que estas no podrán ser transferidas, prestadas, compartidas o utilizadas por terceros. El sistema deberá permitir:

- Emisión
- Activación
- Modificación
- Suspensión
- Bloqueo
- Renovación
- Cancelación
- Recuperación
- Auditoría

Cuando una persona deje de prestar servicios, sea trasladada, suspendida o cambie de funciones, deberá revisarse inmediatamente su autorización de acceso.

7. Control de entrada y salida del personal

El ingreso y salida del personal penitenciario deberá quedar registrado mediante mecanismos confiables. Como mínimo deberá registrarse:

- Identidad
- Fecha
- Hora
- Punto de acceso
- Condición de autorización
- Incidencias relevantes

El sistema deberá impedir que una persona pueda aparecer simultáneamente como presente y ausente en áreas incompatibles, salvo que exista una explicación operacional documentada. Las inconsistencias deberán generar alertas para revisión.

8. Control de visitantes

Los visitantes deberán someterse a un sistema de registro previo o en el punto de acceso, conforme a las normas penitenciarias aplicables. El sistema deberá permitir:

- Identificación

RD Propone RD Propone

- Autorización
- Registro de entrada
- Registro de salida
- Area autorizada
- Horario
- Responsable de la visita cuando corresponda
- Incidencias
- Bienes o equipos autorizados

La información deberá utilizarse exclusivamente para fines legítimos de seguridad, administración penitenciaria e investigación cuando corresponda.

9. Abogados, representantes consulares y otras personas con funciones protegidas

El sistema deberá garantizar controles de seguridad compatibles con las funciones especiales reconocidas por el ordenamiento jurídico a:

- Abogados
- Defensores públicos
- Representantes consulares
- Organismos de derechos humanos
- Autoridades judiciales
- Fiscales
- Personal médico
- Organismos autorizados de supervisión

Los controles no podrán utilizarse para impedir, obstaculizar o vulnerar comunicaciones o actuaciones protegidas por la ley. La condición especial de una persona no significará ausencia de controles de seguridad, sino controles compatibles con sus derechos y funciones legalmente reconocidas.

10. Contratistas y proveedores

Todo contratista, proveedor o técnico externo deberá contar con autorización previa cuando corresponda. La autorización deberá identificar:

- Persona
- Empresa
- Motivo de entrada

RD Propone RD Propone

- Area
- Fecha
- Horario
- Trabajo autorizado
- Herramientas o equipos autorizados
- Responsable institucional

Los permisos deberán ser preferiblemente temporales y vinculados a una orden de trabajo específica.

11. Control de vehículos

Los vehículos que ingresen a establecimientos penitenciarios deberán estar sujetos a controles proporcionales al riesgo. El sistema deberá permitir registrar:

- Placa
- Identificación del conductor
- Empresa o institución
- Motivo del ingreso
- Fecha y hora
- Area de destino
- Bienes transportados
- Autorización correspondiente
- Salida

Los vehículos que transporten alimentos, materiales, equipos, medicamentos, herramientas, combustible u otros bienes deberán contar con documentación y trazabilidad suficiente.

12. Control de bienes, paquetes y mercancías

Todo bien que ingrese a un establecimiento deberá corresponder a una finalidad autorizada. Cuando corresponda, deberá registrarse:

- Descripción
- Cantidad
- Origen
- Destinatario
- Responsable

RD Propone RD Propone

- Fecha
- Autorización
- Comprobante o documento de respaldo
- Salida o destino final

Los sistemas de seguridad deberán prestar especial atención a bienes que, por sus características, puedan facilitar la introducción de dispositivos electrónicos, herramientas no autorizadas u otros objetos prohibidos.

13. Herramientas y equipos de trabajo

Las herramientas y equipos utilizados por personal técnico o contratistas deberán registrarse cuando su naturaleza o el nivel de riesgo del área así lo requiera. El registro podrá incluir:

- Identificación del equipo
- Responsable
- Cantidad
- Estado
- Hora de entrada
- Srea de utilización
- Hora de devolución o salida.

Las herramientas deberán permanecer vinculadas a la orden de trabajo correspondiente.

La pérdida de una herramienta, equipo o componente deberá ser reportada inmediatamente.

14. Dispositivos electrónicos

Los teléfonos celulares, computadoras, tabletas, radios, relojes inteligentes, dispositivos de almacenamiento y otros equipos electrónicos que pretendan ingresar deberán clasificarse como:

a) Autorizados
b) Autorizados temporalmente
c) Institucionales
d) Sujetos a custodia durante la permanencia
e) No autorizados

RD Propone RD Propone

Cada establecimiento deberá disponer de procedimientos claros sobre cuáles dispositivos pueden ingresar y bajo qué condiciones.

La autorización de un dispositivo deberá estar vinculada, cuando resulte técnicamente viable y jurídicamente procedente, con:

- Persona responsable
- Institución
- Finalidad
- Período de autorización
- Zona de utilización

15. Dispositivos temporales

Cuando una persona necesite introducir temporalmente un equipo electrónico por razones laborales, técnicas, médicas, administrativas o institucionales, deberá existir una autorización específica.

Al finalizar la actividad deberá verificarse su salida.

Los dispositivos temporales no deberán convertirse en una excepción permanente.

16. Sistemas de custodia de dispositivos

Los establecimientos deberán disponer de mecanismos seguros para la custodia temporal de dispositivos no autorizados. Estos mecanismos deberán:

- Identificar al propietario
- Registrar la entrega
- Registrar la devolución
- Impedir accesos no autorizados
- Proteger el dispositivo contra pérdida o daño
- Generar trazabilidad

Cuando la custodia corresponda a un dispositivo institucional, deberá existir además responsabilidad formal sobre su manejo.

17. Inspecciones y registros

Las inspecciones, registros, cacheos y requisas deberán realizarse de acuerdo con la Constitución, la legislación penitenciaria, las decisiones judiciales aplicables y los reglamentos correspondientes.

RD Propone RD Propone

La tecnología podrá asistir en la detección y prevención, pero no podrá utilizarse para sustituir las garantías legales.

Toda inspección deberá observar, según corresponda:

- Necesidad
- Proporcionalidad
- Dignidad
- Privacidad
- Documentación
- Responsabilidad del personal actuante
- Cadena de custodia cuando exista evidencia

18. Control de acceso a áreas críticas

Las áreas críticas deberán contar con mecanismos reforzados de autenticación. Cuando el nivel de riesgo lo justifique podrán utilizarse combinaciones de:

- Credencial
- Identificación personal
- Biometría
- Segundo factor
- Autorización temporal
- Acompañamiento
- Registro audiovisual

Ningún mecanismo podrá considerarse suficiente por sí solo para todos los escenarios.

19. Acceso de dos personas a determinadas áreas

En áreas particularmente sensibles podrá establecerse el principio de doble control.

Este principio implica que determinadas operaciones críticas requieran la participación o validación de dos personas autorizadas. Podrá aplicarse, según la evaluación de riesgos, a:

- Centros de monitoreo
- Depósitos de evidencias
- Infraestructura tecnológica crítica
- Sistemas de comunicaciones
- Areas de servidores

RD Propone RD Propone

- Almacenes de dispositivos
- Determinadas operaciones de mantenimiento

La finalidad será reducir el riesgo de manipulación unilateral y aumentar la trazabilidad.

20. Movilidad interna

No se pretende registrar indiscriminadamente cada movimiento de cada persona, sino establecer trazabilidad reforzada en:

- Areas críticas
- Desplazamientos autorizados
- Operaciones especiales
- Mantenimiento
- Traslado de bienes
- Manejo de evidencias
- Incidentes de seguridad

La intensidad del control deberá corresponder al nivel de riesgo.

21. Acompañamiento y escolta interna

Cuando una persona externa deba acceder a una zona restringida y no posea autorización autónoma, podrá requerirse acompañamiento de personal autorizado. El acompañamiento deberá registrarse cuando corresponda.

El responsable del acompañamiento deberá responder por el cumplimiento de la ruta, finalidad y tiempo autorizado, sin asumir funciones que correspondan a otras áreas.

22. Accesos de emergencia

Los protocolos de emergencia deberán garantizar que bomberos, personal médico, protección civil, técnicos esenciales y demás organismos autorizados puedan ingresar rápidamente cuando exista una amenaza para la vida o la integridad física.

Los controles de emergencia deberán ser posteriormente documentados y auditados. La emergencia no eliminará la obligación de registrar el acceso.

23. Pérdida, robo o uso indebido de credenciales

La pérdida o sospecha de compromiso de una credencial deberá generar su bloqueo inmediato cuando técnicamente sea posible. El incidente deberá registrarse.

RD Propone RD Propone

Cuando exista evidencia de utilización indebida, se deberá investigar:

- Quién utilizó la credencial
- Cuándo
- Dónde
- Bajo qué circunstancias
- Si hubo complicidad
- Si existieron fallas de control

24. Alertas de acceso

El sistema podrá generar alertas ante situaciones como:

- Credencial utilizada fuera del horario autorizado
- Intento de acceso a zona no autorizada
- Utilización de una credencial suspendida
- Inconsistencias entre registros
- Accesos incompatibles con la función
- Permanencias anómalas
- Intentos repetidos de acceso no autorizado
- Utilización de credenciales en circunstancias que requieran revisión

Las alertas deberán ser revisadas por personal autorizado.

Ninguna alerta automatizada constituirá por sí misma prueba concluyente de una infracción.

25. Integración con videovigilancia

Los sistemas de control de acceso podrán integrarse con los sistemas de videovigilancia para permitir la verificación de eventos. La integración deberá permitir, cuando corresponda:

ACCESO / IDENTIDAD / HORA / ZONA / REGISTRO VISUAL / EVENTO / REVISIÓN.

Esta integración deberá estar sometida a controles de acceso, auditoría, protección de datos y reglas de conservación de información.

26. Correlación con otros sistemas de seguridad

Cuando sea legal y técnicamente procedente, la información de acceso podrá correlacionarse con:

RD Propone RD Propone

- Incidentes
- Alarmas
- Registros de visitantes
- Inventarios
- Dispositivos autorizados
- Ordenes de mantenimiento
- Sistemas de comunicaciones institucionales
- Registros de vehículos
- Controles de herramientas
- Investigaciones

La finalidad será detectar inconsistencias y facilitar la reconstrucción de acontecimientos.

27. Trazabilidad de órdenes de trabajo

Toda intervención técnica relevante dentro de áreas restringidas deberá estar vinculada a una orden de trabajo, la que deberá indicar al menos lo siguiente:

- Finalidad
- Personal autorizado
- Empresa
- Area
- Fecha
- Horario
- Equipos
- Herramientas
- Responsable institucional

Cuando la intervención termine, deberá registrarse su conclusión.

28. Control de mantenimiento

Las actividades de mantenimiento de infraestructura física, eléctrica, tecnológica y de comunicaciones deberán someterse a controles reforzados cuando puedan afectar sistemas críticos.

El personal técnico no deberá tener acceso permanente a instalaciones o sistemas simplemente por haber intervenido anteriormente en ellos.

29. Control de paquetes y entregas

RD Propone RD Propone

Los paquetes destinados al establecimiento deberán contar con mecanismos de recepción, inspección, registro y distribución. Cuando corresponda, deberán registrarse:

- Remitente
- Transportista
- Destinatario
- Contenido declarado
- Autorización
- Fecha
- Hora
- Responsable de recepción
- Destino

Las excepciones relacionadas con medicamentos, documentos jurídicos, correspondencia protegida u otros bienes sujetos a régimen especial deberán ser reguladas de manera específica.

30. Prohibición de accesos informales

Queda prohibido establecer accesos permanentes basados exclusivamente en:

- Relaciones personales
- Instrucciones verbales no registradas
- Costumbre
- Antigüedad
- Confianza informal
- Autorizaciones genéricas sin fundamento

Toda excepción deberá quedar documentada y ser susceptible de auditoría.

31. Protección de datos

Los registros de acceso constituyen información institucional sensible y por tal razón su tratamiento deberá observar:

- Finalidad determinada
- Acceso restringido
- Seguridad
- Integridad
- Conservación limitada

RD Propone RD Propone

- Trazabilidad
- Eliminación o anonimización cuando corresponda
- Respeto de los derechos reconocidos por la legislación

El personal no podrá consultar información de movimientos por curiosidad, interés personal o finalidad ajena a sus funciones.

32. Acceso a los registros

El acceso a los registros deberá organizarse bajo el principio de necesidad de conocimiento. Cada consulta relevante deberá quedar registrada.

Deberá ser posible determinar:

quién consultó la información, cuándo, qué sistema utilizó y bajo qué autorización.

33. Conservación de registros

Los períodos de conservación deberán definirse de acuerdo con:

- Finalidad
- Valor operacional
- Obligaciones legales
- Investigaciones
- Procesos judiciales
- Necesidades de auditoría
- Protección de datos
- Capacidad tecnológica

Cuando exista una investigación o proceso en curso, los registros relevantes deberán preservarse conforme a las reglas aplicables.

34. Integridad de los registros

Los sistemas deberán incorporar mecanismos que permitan detectar alteraciones no autorizadas. Los registros críticos deberán contar con mecanismos de:

- Integridad
- Sellado temporal
- Auditoría
- Respaldo
- Control de modificaciones

RD Propone RD Propone

La modificación de un registro histórico deberá generar evidencia de la modificación y de la persona autorizada que la realizó.

35. Evidencia derivada de los sistemas de acceso

Cuando un registro de acceso pueda tener relevancia investigativa, deberá preservarse conforme a las reglas de evidencia y cadena de custodia aplicables.

La existencia de un registro electrónico no significa automáticamente que pueda utilizarse sin verificar:

- Autenticidad
- Integridad
- 0rigen
- Contexto
- Confiabilidad
- Forma de obtención

36. Prohibición de vigilancia indiscriminada

El Sistema no podrá convertirse en un mecanismo de vigilancia general e ilimitada. Los controles deberán estar vinculados a finalidades legítimas de:

- Seguridad
- Administración penitenciaria
- Prevención
- Protección de personas
- Investigación legalmente autorizada
- Respuesta a incidentes

No podrán utilizarse para discriminación, persecución personal, represalias o intereses ajenos a las funciones institucionales.

37. No discriminación y tratamiento igualitario

No podrán establecerse controles diferenciados exclusivamente por:

- Origen
- Nacionalidad
- Sexo
- Religión

RD Propone RD Propone

- Opinión
- Condición social
- Apariencia
- Discapacidad
- Orientación política
- Cualquier otra condición protegida por el ordenamiento jurídico

Las diferencias deberán justificarse por funciones, riesgos o circunstancias objetivas.

38. Sistema de autorización temporal

El Sistema deberá permitir emitir autorizaciones con fecha y hora de inicio y terminación. Esto será particularmente útil para:

- Contratistas
- Técnicos
- Proveedores
- Visitas especiales
- Organismos externos
- Investigadores
- Actividades académicas
- Mantenimiento
- Inspecciones

Una autorización temporal deberá expirar automáticamente cuando técnicamente sea posible.

39. Integración con el Centro Nacional de Monitoreo

Los eventos relevantes de acceso deberán poder integrarse con el Centro Nacional de Monitoreo, Inteligencia y Análisis Penitenciario. El Centro podrá recibir:

- Alertas
- Incidencias
- Accesos críticos
- Inconsistencias
- Pérdida de credenciales
- Accesos extraordinarios
- Eventos vinculados a investigaciones

RD Propone RD Propone

La integración no convertirá al Centro Nacional en autoridad disciplinaria o judicial, su función será apoyar la detección, coordinación, análisis y generación de información para las autoridades competentes.

40. Auditorías periódicas

Las auditorías deberán verificar, como mínimo:

- funcionamiento de credenciales;
- registros;
- cámaras;
- controles de visitantes;
- vehículos;
- bienes;
- herramientas;
- dispositivos electrónicos;
- áreas críticas;
- permisos temporales;
- accesos de emergencia;
- registros de mantenimiento;
- integridad de la información.

Las deficiencias deberán generar planes correctivos.

41. Pruebas de funcionamiento

Los sistemas de control deberán someterse a pruebas programadas y aleatorias. Las pruebas deberán verificar que:

- Una credencial cancelada no continúe funcionando
- Una autorización temporal expire
- Los registros correspondan a los eventos reales
- Las cámaras permitan verificar los accesos relevantes
- Los sistemas mantengan continuidad
- Las alertas lleguen al personal responsable
- Los mecanismos de respaldo funcionen

Las pruebas deberán documentarse.

42. Régimen de excepciones

RD Propone RD Propone

Toda excepción a los controles ordinarios deberá:

1. Tener fundamento
2. Identificar al responsable
3. Establecer duración
4. Indicar alcance
5. Quedar registrada
6. Ser revisable
7. Ser auditada cuando corresponda

Las excepciones no podrán convertirse en mecanismos permanentes de elusión de controles.

43. Incidentes relacionados con el acceso

Cuando se detecte un acceso irregular, el establecimiento deberá activar el protocolo correspondiente. Deberán preservarse, cuando corresponda:

- Registros de acceso
- Imágenes
- Autorizaciones;
- Ordenes de trabajo
- Registros de dispositivos
- Información de vehículos
- Registros de bienes
- Comunicaciones institucionales relacionadas
- Cualquier otra evidencia pertinente

La investigación deberá determinar si el incidente fue producto de:

- Error
- Falla tecnológica
- Deficiencia procedimental
- Negligencia
- Manipulación
- Fraude
- Corrupción
- Complicidad
- Vulnerabilidad del sistema

RD Propone RD Propone

44. Responsabilidad del personal

El personal responsable de controles de acceso deberá cumplir estrictamente los procedimientos establecidos. Se diferenciarán:

a) Error operacional
b) Negligencia
c) Incumplimiento deliberado
d) Alteración de registros
e) Facilitación
f) Encubrimiento
g) Participación en actividades ilícitas

La responsabilidad deberá determinarse mediante el procedimiento correspondiente y respetando el debido proceso.

45. Capacitación específica

Todo personal que administre o utilice sistemas de control de acceso deberá recibir capacitación sobre:

- Identificación
- Credenciales
- Control de visitantes
- Dispositivos electrónicos
- Herramientas
- Bienes
- Protección de datos
- Seguridad tecnológica
- Cadena de custodia
- Respuesta ante incidentes
- Derechos fundamentales
- Prevención de corrupción
- Responsabilidades disciplinarias y legales

El acceso a funciones críticas deberá estar condicionado a la capacitación y certificación correspondiente.

46. Indicadores nacionales

RD Propone RD Propone

El Sistema deberá medir, como mínimo:

- Número de accesos
- Accesos no autorizados
- Intentos de acceso
- Credenciales suspendidas utilizadas
- Credenciales perdidas
- Incidencias de visitantes
- Incidencias de proveedores
- Vehículos inspeccionados
- Bienes registrados
- Herramientas extraviadas
- Dispositivos no autorizados detectados
- Alertas generadas
- Alertas confirmadas
- Falsos positivos
- Tiempo de respuesta
- Fallas tecnológicas
- Disponibilidad del sistema
- Incumplimientos detectados
- Acciones correctivas

Los indicadores deberán utilizarse para mejorar el sistema y no únicamente para producir estadísticas.

47. Indicadores de eficiencia

El sistema deberá medir también el costo de los controles frente a los resultados obtenidos. Deberán evaluarse:

- Costo por establecimiento
- Costo de mantenimiento
- Disponibilidad tecnológica
- Reducción de incidentes
- Tiempos de respuesta
- Número de controles efectivos
- Carga operacional
- Porcentaje de controles automatizados

RD Propone RD Propone

- Necesidad de intervención humana
- Costo de reposición
- Vida útil de los equipos

El objetivo será evitar sistemas costosos que produzcan poca utilidad operacional.

48. Interoperabilidad

Los sistemas de control de acceso deberán diseñarse bajo estándares que permitan su integración progresiva con los demás componentes del Sistema Nacional de Seguridad Penitenciaria.

No deberán crearse plataformas aisladas que obliguen al Estado a mantener múltiples registros incompatibles. La interoperabilidad deberá respetar:

- Seguridad
- Privacidad
- Competencias institucionales
- Control de acceso
- Integridad
- Trazabilidad

49. Independencia tecnológica

Las soluciones tecnológicas deberán evitar dependencias innecesarias de un proveedor, los contratos deberán contemplar, cuando corresponda:

- Documentación técnica
- Transferencia de conocimiento
- Respaldo de información
- Portabilidad
- Continuidad
- Mantenimiento
- Actualización
- Mecanismos de sustitución
- Recuperación de información al finalizar el contrato

El Estado deberá conservar la capacidad de administrar sus propios registros y sistemas.

50. Integración con la seguridad física

RD Propone RD Propone

La tecnología no sustituirá:

- Puertas
- Cerraduras
- Barreras
- Iluminación
- Vigilancia
- Procedimientos
- Personal
- Protocolos de emergencia

El sistema deberá concebirse como una arquitectura de defensa en profundidad. La seguridad deberá funcionar mediante capas complementarias.

51. Principio de trazabilidad completa

Todo proceso crítico deberá procurar la siguiente secuencia:

PERSONA / VEHÍCULO / BIEN / EQUIPO – IDENTIFICACIÓN – AUTORIZACIÓN – CONTROL – REGISTRO – MOVILIDAD – SUPERVISIÓN – SALIDA - AUDITORÍA

Cuando una etapa crítica no pueda ser verificada, deberá generarse una alerta administrativa o de seguridad según corresponda.

52. Relación con la prevención del ingreso de teléfonos clandestinos

El control de acceso constituye una de las primeras barreras contra la introducción de teléfonos celulares y otros dispositivos de comunicación no autorizados. Por ello, la política nacional deberá evitar depender exclusivamente de tecnologías posteriores de detección.

La estrategia deberá combinar:

CONTROL DE PERSONAS + CONTROL DE BIENES + CONTROL DE VEHÍCULOS + CONTROL DE DISPOSITIVOS + VIGILANCIA + INTELIGENCIA + INVESTIGACIÓN.

La prevención del ingreso deberá ser considerada preferible a depender exclusivamente de la detección posterior.

53. Relación con la corrupción y la complicidad interna

Los registros de acceso deberán utilizarse, cuando legalmente corresponda, para identificar patrones que puedan indicar:

RD Propone RD Propone

- Accesos atípicos
- Repetición de excepciones
- Autorizaciones injustificadas
- Interacción irregular entre personas
- Manipulación de registros
- Ingreso de terceros fuera de procedimientos
- Desaparición de bienes
- Utilización irregular de herramientas
- Incumplimiento sistemático de controles

Estos elementos podrán alimentar análisis administrativos o investigativos, pero no podrán convertirse automáticamente en una imputación de responsabilidad.

54. Protección de los trabajadores y visitantes

El sistema también tendrá como finalidad proteger al personal penitenciario, visitantes, abogados, proveedores, profesionales de la salud y demás personas autorizadas.

Un buen sistema de control no solamente evita que entren objetos prohibidos. También permite:

- Conocer quién está dentro del establecimiento
- Localizar personas durante una emergencia
- Acelerar evacuaciones
- Identificar áreas afectadas
- Facilitar respuestas médicas
- Reconstruir incidentes

La seguridad penitenciaria deberá proteger simultáneamente a la institución y a las personas.

55. Evaluación independiente

La implementación nacional deberá ser evaluada periódicamente por órganos internos y, cuando corresponda, por evaluadores externos independientes.

56. Revisión después de incidentes

Todo incidente grave relacionado con acceso, movilidad, ingreso de objetos prohibidos o utilización indebida de credenciales deberá generar una revisión posterior. La revisión deberá identificar:

RD Propone RD Propone

- Qué ocurrió
- Cómo ocurrió
- Qué controles existían
- Cuáles funcionaron
- Cuáles fallaron
- Por qué fallaron
- Qué modificaciones deben realizarse.\

El objetivo será corregir vulnerabilidades sistémicas y no limitarse a atribuir responsabilidad individual.

57. Banco Nacional de vulnerabilidades

El Ministerio de Justicia deberá mantener un registro nacional de vulnerabilidades relacionadas con accesos, credenciales, visitantes, vehículos, proveedores, bienes, dispositivos, herramientas, sistemas tecnológicos e infraestructura.

Las vulnerabilidades recurrentes deberán convertirse en prioridades nacionales de corrección.

58. Coordinación con la contratación pública

Las adquisiciones vinculadas al Sistema Nacional de Control de Acceso deberán planificarse conforme al marco vigente de contratación pública. Las especificaciones deberán priorizar:

- Necesidad real
- Interoperabilidad
- Costo total de propiedad
- Mantenimiento
- Seguridad
- Disponibilidad
- Escalabilidad
- Vida útil
- Transferencia de conocimiento
- Ausencia de dependencia tecnológica injustificada

Las compras deberán orientarse a resolver capacidades identificadas y no simplemente a adquirir equipos.

RD Propone RD Propone

59. Implementación progresiva

La implementación podrá desarrollarse por fases:

FASE I: Diagnóstico nacional.

FASE II: Clasificación de áreas y riesgos.

FASE III: Normalización de credenciales y registros.

FASE IV: Control de visitantes, vehículos y bienes.

FASE V: Integración tecnológica.

FASE VI: Incorporación de áreas críticas.

FASE VII: Interoperabilidad nacional.

FASE VIII: Evaluación y optimización.

La implementación deberá comenzar prioritariamente en establecimientos y áreas donde la evaluación de riesgo determine mayor exposición.

60. Responsabilidad institucional

El Ministerio de Justicia: establecerá las políticas y normas generales del Sistema, conforme al marco legal vigente.

La Dirección General de Servicios Penitenciarios y Correccionales: será responsable de la implementación operacional dentro de sus competencias.

Las demás instituciones participantes ejercerán sus funciones conforme al ordenamiento jurídico.

La responsabilidad deberá estar claramente distribuida para evitar que una falla termine siendo atribuida genéricamente a "el sistema".

61. Principio rector del capítulo

El Estado deberá procurar que ninguna persona, vehículo, bien o equipo pueda ingresar, circular o permanecer dentro de un establecimiento penitenciario sin que exista una razón legítima, una autorización compatible con esa razón y un nivel de trazabilidad proporcional al riesgo.

RD Propone RD Propone

La seguridad penitenciaria moderna no consiste en controlar todo indiscriminadamente, consiste en saber qué debe controlarse, por qué debe controlarse, quién está autorizado, quién es responsable y qué ocurrió cuando el control fue activado.

62. Fórmula operacional

El Sistema Nacional deberá estructurarse bajo la siguiente lógica:

IDENTIFICAR - AUTORIZAR - CONTROLAR - REGISTRAR - SUPERVISAR - DETECTAR - RESPONDER - INVESTIGAR - CORREGIR - AUDITAR.

Esta cadena deberá integrarse con los sistemas de comunicaciones, videovigilancia, inteligencia penitenciaria, gestión de incidentes, ciberseguridad, capacitación, contratación tecnológica y evaluación nacional establecidos en los capítulos precedentes.

CAPÍTULO XXV
SISTEMA NACIONAL DE CONTROL DE BIENES, PAQUETES, ALIMENTOS, HERRAMIENTAS, SUMINISTROS Y LOGÍSTICA PENITENCIARIA

1. Objeto

El presente capítulo establece las normas generales para controlar el ingreso, recepción, almacenamiento, distribución, utilización y salida de bienes dentro del Sistema Penitenciario.

Su finalidad será reducir las oportunidades de introducir objetos prohibidos, dispositivos de comunicación, herramientas no autorizadas, sustancias, componentes tecnológicos u otros elementos capaces de comprometer la seguridad.

2. Principio de trazabilidad logística

Todo bien considerado crítico deberá poder ser asociado, según corresponda, con:

ORIGEN - TRANSPORTE - RECEPCIÓN - INSPECCIÓN - ALMACENAMIENTO - ENTREGA - UTILIZACIÓN - DEVOLUCIÓN/SALIDA.

La inexistencia de trazabilidad en una operación crítica deberá considerarse una vulnerabilidad institucional.

3. Clasificación de bienes

Los establecimientos deberán clasificar los bienes, como mínimo, en:

a) Alimentos

RD Propone RDPropone

b) Medicamentos
c) Materiales de limpieza
d) Herramientas
e) Equipos electrónicos
f) Equipos de comunicación
g) Materiales de construcción
h) Suministros administrativos
i) Bienes destinados a personas privadas de libertad
j) Bienes institucionales
k) Bienes de terceros
l) Bienes sujetos a custodia especial

4. Recepción de mercancías

La recepción deberá realizarse en áreas designadas. Cuando corresponda se verificará:

- Identidad del transportista
- Vehículo
- Documentación
- Cantidad
- Descripción
- Destinatario
- Estado del embalaje
- Autorización
- Fecha y hora

5. Inspección

Los bienes deberán ser inspeccionados mediante procedimientos compatibles con su naturaleza y con el nivel de riesgo.

Podrán utilizarse:

- Inspección visual
- Revisión documental
- Sistemas tecnológicos de inspección
- Pesaje
- Conteo
- Verificación de integridad

RD Propone RD Propone

- Otros mecanismos legalmente autorizados

6. Bienes de alto riesgo

Los bienes que puedan facilitar la introducción de dispositivos de comunicación, herramientas de evasión, componentes tecnológicos o elementos peligrosos deberán recibir controles reforzados.

7. Herramientas

Las herramientas destinadas a talleres, mantenimiento o construcción deberán permanecer asociadas a inventarios y responsables.

Las pérdidas deberán ser reportadas inmediatamente.

8. Componentes tecnológicos

Todo componente electrónico destinado a infraestructura penitenciaria deberá estar registrado cuando su naturaleza lo amerite. Se prestará especial atención a:

- Teléfonos
- Radios
- Módems
- Routers
- Dispositivos de almacenamiento
- Baterías
- Cargadores
- Componentes de redes
- Equipos de transmisión

25.9. Almacenes

Los almacenes deberán contar con control de acceso, inventario, responsables definidos, registros de entrada y salida, controles periódicos y conciliaciones.

10. Inventarios

Los inventarios deberán permitir comparar:

existencia física + registros administrativos + movimientos registrados.

Las diferencias deberán investigarse.

11. Alimentos

RD Propone RD Propone

Los alimentos destinados a establecimientos penitenciarios deberán estar sujetos a controles de recepción, almacenamiento y distribución.

Las inspecciones deberán realizarse respetando las normas sanitarias y los derechos aplicables.

12. Medicamentos

Los medicamentos deberán contar con controles reforzados debido a su importancia para la salud y al riesgo de desvío.

13. Paquetes destinados a personas privadas de libertad

Los paquetes autorizados deberán someterse al régimen establecido para su categoría.

La existencia de controles de seguridad no podrá utilizarse para vulnerar comunicaciones o documentos jurídicamente protegidos.

14. Correspondencia protegida

La correspondencia sujeta a protección legal deberá recibir un tratamiento diferenciado.

Los mecanismos de seguridad deberán impedir que las excepciones sean utilizadas como mecanismo general para introducir objetos prohibidos, sin desconocer las garantías correspondientes.

15. Transporte

Los vehículos utilizados para abastecimiento deberán quedar vinculados a las entregas realizadas.

16. Proveedores

Los proveedores deberán cumplir los protocolos de seguridad del establecimiento.

El incumplimiento podrá generar consecuencias contractuales, administrativas o legales según corresponda.

17. Control de devolución

Las herramientas, equipos y materiales temporales deberán registrarse también al momento de su devolución o salida.

18. Pérdidas

RD Propone RD Propone

Toda pérdida deberá generar:

1. Reporte
2. Verificación
3. Investigación cuando corresponda
4. Determinación de responsabilidad
5. Corrección del control que permitió la pérdida

19. Conciliación

Los inventarios críticos deberán ser conciliados periódicamente.

20. Auditoría logística

La auditoría deberá verificar:

- Inventarios
- Proveedores
- Ordenes
- Entregas
- Pérdidas
- Devoluciones
- Accesos
- Registros tecnológicos

21. Integración tecnológica

La información logística podrá integrarse con:

- Control de acceso
- Videovigilancia
- Incidentes
- Inteligencia
- Contrataciones
- Inventarios
- Investigaciones

CAPÍTULO XXVI
SEGURIDAD FÍSICA, PERIMETRAL, INFRAESTRUCTURA CRÍTICA Y RESILIENCIA DEL ESTABLECIMIENTO PENITENCIARIO

RD Propone RD Propone

1. Objeto

Este capítulo establece los criterios nacionales de seguridad física y protección de infraestructura penitenciaria.

2. Defensa en profundidad

La seguridad deberá combinar:

- Perímetro
- Accesos
- Iluminación
- Cerramientos
- Puertas
- Controles internos
- Videovigilancia
- Alarmas
- Comunicaciones
- Energía
- Personal
- Procedimientos

3. Evaluación de vulnerabilidades

Cada establecimiento deberá realizar evaluaciones periódicas de:

- Perímetro
- Accesos
- Techos
- Muros
- Ventanas
- Túneles o espacios ocultos
- Redes
- Infraestructura eléctrica
- Sistemas tecnológicos
- Zonas de baja visibilidad

4. Iluminación

RD Propone RD Propone

Las zonas críticas deberán contar con iluminación suficiente y sistemas de respaldo cuando sea necesario.

5. Videovigilancia

La videovigilancia deberá cubrir prioritariamente:

- Accesos
- Perímetro
- Zonas críticas
- Almacenes
- Areas tecnológicas
- Puntos de recepción
- Areas de circulación relevantes

La instalación deberá evitar espacios donde exista una expectativa legítima de privacidad incompatible con la vigilancia.

6. Integridad de cámaras

El sistema deberá detectar:

- Pérdida de señal
- Manipulación
- Obstrucción
- Desconexión
- Alteraciones
- Fallas

7. Infraestructura eléctrica

La infraestructura eléctrica deberá diseñarse prioritariamente para:

- Seguridad
- Continuida
- Prevención de incendios
- Protección de personas
- Estabilidad tecnológica
- Detección de anomalías

RD Propone RD Propone

Queda excluido como política institucional el uso deliberado de energía eléctrica para destruir o dañar teléfonos u otros dispositivos.

8. Respaldo energético

Los sistemas críticos deberán contar con mecanismos de continuidad adecuados al nivel de riesgo.

9. Protección de salas tecnológicas

Las salas de servidores, telecomunicaciones y monitoreo deberán tener controles reforzados.

10. Protección contra incendios

La infraestructura deberá incorporar sistemas de prevención, detección y respuesta contra incendios.

11. Agua y servicios esenciales

Los establecimientos deberán disponer de planes de continuidad para:

- Agua
- Energía
- Comunicaciones
- Alimentación
- Atención médica
- Saneamiento

12. Mantenimiento

Las fallas estructurales o tecnológicas críticas deberán clasificarse por prioridad.

13. Tiempos máximos de atención

Los contratos de mantenimiento deberán establecer tiempos máximos razonables de respuesta según criticidad.

14. Vulnerabilidades temporales

Cuando una infraestructura crítica no pueda repararse inmediatamente deberán establecerse medidas compensatorias.

15. Obras nuevas

RD Propone RD Propone

Todo nuevo establecimiento deberá incorporar seguridad desde la fase de diseño.

16. Remodelaciones

Las remodelaciones deberán incluir evaluación de seguridad antes de su aprobación.

17. Prohibición de puntos ciegos críticos

Las zonas donde una persona pueda introducir, ocultar o intercambiar bienes prohibidos deberán ser identificadas y reducidas progresivamente.

18. Mantenimiento de vegetación

Las áreas exteriores deberán mantenerse de manera que no generen obstáculos a la vigilancia.

19. Drenajes y estructuras subterráneas

Las estructuras que puedan comprometer la seguridad deberán incluirse en las inspecciones periódicas.

CAPÍTULO XXVII
PREVENCIÓN INTEGRAL DE LA CORRUPCIÓN, LA COMPLICIDAD Y LA CAPTURA OPERATIVA DEL SISTEMA PENITENCIARIO

1. Objeto

Este capítulo establece mecanismos para reducir el riesgo de corrupción y complicidad interna.

2. Principio

La seguridad tecnológica será insuficiente si una persona autorizada puede facilitar deliberadamente la entrada o utilización de medios prohibidos.

3. Riesgos

Se considerarán riesgos, entre otros:

- Introducción de teléfonos
- Ingreso de sustancias
- Alteración de registros
- Acceso irregular
- Filtración de información

RD Propone RD Propone

- Manipulación de cámaras
- Manipulación de sistemas
- Favorecimiento de personas privadas de libertad
- Recepción de pagos indebidos

4. Declaración de conflictos

El personal deberá declarar situaciones que puedan comprometer su imparcialidad conforme a las normas aplicables.

5. Rotación

Podrán utilizarse mecanismos de rotación en posiciones particularmente expuestas cuando la evaluación de riesgo lo justifique.

6. Separación de funciones

Las funciones críticas deberán distribuirse para reducir la posibilidad de manipulación unilateral.

7. Doble control

Las operaciones especialmente sensibles podrán requerir dos funcionarios autorizados.

8. Canal de denuncias

Deberán existir canales seguros para reportar:

- Corrupción
- Amenazas
- Presiones
- Introducción de dispositivos
- Complicidad
- Alteración de registros

9. Protección del denunciante

Las personas que reporten de buena fe deberán recibir protección frente a represalias conforme al ordenamiento jurídico.

10. Análisis patrimonial

Cuando existan indicios legalmente relevantes, las autoridades competentes podrán activar los mecanismos de investigación patrimonial establecidos por la legislación.

RD Propone RD Propone

11. Acceso a sistemas

El personal deberá tener únicamente los permisos necesarios.

12. Auditoría de usuarios

Las consultas y modificaciones de sistemas críticos deberán quedar registradas.

13. Conductas de alto riesgo

Deberán recibir atención especial:

- Uso de credenciales ajenas
- Eliminación de registros
- Desactivación injustificada de cámaras
- Ingreso fuera de horario
- Excepciones repetitivas
- Alteraciones de inventario

14. Contratistas

Las empresas externas deberán estar sujetas a controles de integridad y seguridad.

15. Investigación

Los casos deberán remitirse a las autoridades competentes según su naturaleza.

16. Responsabilidad

La responsabilidad deberá diferenciar:

- Error
- Negligencia
- Incumplimiento
- Complicidad
- Participación
- Encubrimiento

17. No represalias

Ninguna persona deberá ser sancionada por formular una denuncia de buena fe por el solo hecho de denunciar.

18. Formación ética

RD Propone RD Propone

La capacitación deberá incluir integridad pública, conflictos de interés, protección de información y responsabilidad profesional.

19. Indicadores

Se medirán:

- Denuncias
- Investigaciones
- Tiempos de respuesta
- Reincidencias
- Areas vulnerables
- Controles implementados

20. Evaluación

Los resultados deberán integrarse al sistema nacional de evaluación.

CAPÍTULO XXVIII
TRANSPARENCIA, RENDICIÓN DE CUENTAS, INFORMACIÓN PÚBLICA Y SUPERVISIÓN SOCIAL

1. Objeto

El Sistema Nacional de Seguridad Penitenciaria deberá operar bajo criterios de transparencia, rendición de cuentas y control institucional, sin comprometer información cuya divulgación pueda afectar legítimamente la seguridad.

2. Información pública

El Estado deberá publicar periódicamente información agregada sobre:

- Incidentes
- Dispositivos clandestinos incautados
- Establecimientos intervenidos
- Capacitación
- Disponibilidad tecnológica
- Auditorías
- Cumplimiento de metas
- Ejecución presupuestaria
- Contrataciones

RD Propone RD Propone

- Resultados

3. Información reservada

No deberá divulgarse información operacional cuya publicación facilite:

- Evasión de controles
- Vulneración tecnológica
- Identificación de fuentes
- Afectación de investigaciones
- Ataques contra infraestructura

4. Equilibrio

La reserva deberá ser excepcional, justificada y limitada.

5. Informes anuales

El Ministerio de Justicia deberá presentar un informe anual sobre la ejecución del Sistema.

6. Contenido mínimo

El informe deberá incluir:

1. Avances
2. Metas
3. Indicadores
4. Presupuesto
5. Auditorías
6. Incidentes agregados
7. Vulnerabilidades corregidas
8. Proyectos en ejecución
9. Resultados de evaluación

7. Contrataciones

Las adquisiciones deberán someterse a las reglas de transparencia y publicidad aplicables. La DGCP mantiene actualmente el marco operativo de la Ley 47-25 y su Reglamento 52-26, incluyendo manuales y mecanismos electrónicos de contratación.

8. Supervisión institucional

Los órganos competentes podrán realizar auditorías, inspecciones y revisiones.

RD Propone RD Propone

9. Supervisión independiente

Podrán realizarse evaluaciones independientes cuando la complejidad o sensibilidad del Sistema lo justifique.

10. Participación académica

El Estado podrá establecer convenios con universidades y centros de investigación para evaluar:

- Tecnología
- Reinserción
- Seguridad
- Eficiencia
- Derechos
- Inteligencia penitenciaria

11. Innovación

Las instituciones podrán realizar proyectos piloto controlados.

12. Proyectos piloto

Todo piloto deberá tener:

- Objetivo
- Duración
- Presupuesto
- Indicadores
- Evaluación
- Criterios de continuidad o terminación

13. Prohibición de expansión automática

Una tecnología piloto no deberá desplegarse nacionalmente únicamente porque haya sido adquirida. Deberá demostrar resultados suficientes.

14. Auditoría ciudadana indirecta

La información agregada deberá permitir a la ciudadanía conocer si el Estado está alcanzando sus objetivos sin exponer vulnerabilidades operacionales.

15. Corrección pública

RD Propone RD Propone

Cuando una evaluación revele deficiencias relevantes, la autoridad deberá establecer un plan de corrección.

CAPÍTULO XXIX
FINANCIAMIENTO, PROGRAMACIÓN PRESUPUESTARIA Y SOSTENIBILIDAD ECONÓMICA

1. Financiamiento

La ejecución del Sistema deberá financiarse mediante las asignaciones presupuestarias correspondientes y demás fuentes legalmente disponibles.

2. Programación plurianual

Las inversiones tecnológicas deberán planificarse considerando su ciclo de vida.

3. Costo total

Toda adquisición deberá considerar:

- Adquisición
- Instalación
- Capacitación
- Licencias
- Mantenimiento
- Actualizaciones
- Sustitución
- Soporte
- Consumo energético
- Retiro

4. Fondo de mantenimiento

El presupuesto deberá contemplar recursos suficientes para mantenimiento de sistemas críticos.

5. Prohibición de tecnología abandonada

No deberá adquirirse tecnología sin prever cómo será mantenida durante su vida útil.

6. Priorización

Cuando existan restricciones presupuestarias se priorizarán:

RD Propone RD Propone

1. Riesgos críticos
2. Continuidad
3. Prevención
4. Detección
5. Respuesta
6. Investigación
7. Modernización

7. Evaluación económica

Los proyectos relevantes deberán someterse a análisis de costo-beneficio o metodología equivalente.

8. Economía

La eficiencia económica deberá buscar el mejor resultado de seguridad posible dentro de los recursos disponibles.

9. Contratación por resultados

Cuando jurídicamente proceda podrán utilizarse mecanismos contractuales vinculados a niveles de servicio y resultados verificables.

10. Evitar dependencia

Los contratos deberán reducir riesgos de dependencia excesiva de un proveedor.

11. Reposición

Deberá existir planificación para sustituir equipos obsoletos.

12. Inventario tecnológico

El Estado deberá mantener inventario de:

- Equipos
- Licencias
- Garantías
- Contratos
- Proveedores
- Fechas de vencimiento
- Vida útil

RD Propone RD Propone

13. Auditoría financiera

La ejecución financiera estará sujeta a los controles establecidos por el ordenamiento.

14. Transparencia

Las inversiones deberán ser publicadas conforme a las reglas aplicables.

15. Cooperación

Podrán gestionarse cooperación técnica o financiera nacional e internacional cuando resulte compatible con las prioridades nacionales y el ordenamiento jurídico.

CAPÍTULO XXX
IMPLEMENTACIÓN NACIONAL, FASES, TRANSICIÓN Y GESTIÓN DEL CAMBIO

1. Fase I - Preparación

Durante la primera fase se realizará:

- Diagnóstico nacional
- Inventario
- Clasificación de establecimientos
- Evaluación de riesgos
- Identificación de brechas
- Definición de indicadores

2. Fase II - Contención inmediata

Se implementarán medidas de bajo costo y alto impacto:

- Revisión de accesos
- Inventarios
- Control de credenciales
- Protocolos
- Capacitación
- Reparación de fallas críticas
- Revisión de dispositivos

3. Fase III - Pilotos tecnológicos

Se seleccionarán establecimientos representativos para probar:

RD Propone RD Propone

- Detección
- Monitoreo
- Control de acceso
- Videovigilancia
- Sistemas de información
- Comunicaciones legítimas

4. Fase IV - Evaluación

Cada piloto deberá ser evaluado antes de su expansión.

5. Fase V - Primera expansión

Se priorizarán establecimientos con mayor nivel de riesgo.

6. Fase VI - Expansión nacional

La implementación se extenderá progresivamente.

7. Fase VII - Optimización

Una vez alcanzada cobertura nacional se procederá a:

- Modernización
- Interoperabilidad
- Sustitución tecnológica
- Evaluación
- Mejora continua

8. Plazos orientativos

El programa nacional podrá estructurarse en un horizonte aproximado de cinco años:

0–6 meses:	Diagnóstico y contención.
6–12 meses:	Pilotos.
12–18 meses:	Evaluación y ajustes.
18–36 meses:	Expansión priorizada.
36–48 meses:	Cobertura ampliada.
48–60 meses:	Consolidación y optimización.

RD Propone RD Propone

9. Continuidad institucional

Los cambios de autoridades no deberán interrumpir proyectos críticos previamente aprobados.

10. Gestión del cambio

La implementación deberá considerar:

- Capacitación
- Comunicación interna
- Adaptación de procesos
- Participación del personal
- Evaluación de resistencia
- Soporte tecnológic

11. No sustitución inmediata

Los sistemas nuevos no deberán reemplazar automáticamente sistemas existentes hasta comprobar que el nuevo mecanismo funciona correctamente.

12. Pruebas de aceptación

Antes de la puesta en producción deberán realizarse pruebas técnicas y operacionales.

13. Criterios de expansión

La expansión deberá considerar:

- Eficacia
- Costo
- Disponibilidad
- Seguridad
- Aceptación operacional
- Impacto sobre derechos
- Sostenibilidad

14. Corrección

Los resultados negativos deberán generar ajustes.

CAPÍTULO XXXI
ARMONIZACIÓN LEGAL, REGLAMENTARIA Y ADMINISTRATIVA

RD Propone RD Propone

1. Armonización

La implementación del presente anteproyecto deberá armonizarse con:

- Constitución de la República
- Legislación penitenciaria
- Legislación penal
- Legislación procesal penal
- Legislación de telecomunicaciones
- Legislación de protección de datos
- Legislación de función pública
- Legislación de contratación pública
- Legislación de archivos
- Normativa sobre transparencia
- Demás disposiciones aplicables

2. Reglamentación

El Poder Ejecutivo, por medio de las autoridades competentes, deberá desarrollar los reglamentos necesarios para la aplicación de esta política dentro del marco constitucional y legal.

3. Protocolos

Las instituciones responsables elaborarán protocolos técnicos y operacionales.

4. Manuales

Los procedimientos deberán ser desarrollados mediante manuales actualizables.

5. Actualización tecnológica

Los protocolos deberán revisarse periódicamente para responder a cambios tecnológicos.

6. Neutralidad tecnológica

La norma no deberá quedar atada a una marca, fabricante o tecnología específica.

7. Evolución normativa

Las referencias a instituciones, tecnologías o procedimientos deberán interpretarse de manera compatible con futuras reformas legales.

8. Competencias

RD Propone RD Propone

Ninguna disposición del presente anteproyecto deberá interpretarse como transferencia automática de competencias constitucionales o legales entre instituciones.

9. Ministerio Público

Las investigaciones penales continuarán correspondiendo a las autoridades competentes conforme al ordenamiento jurídico.

10. Poder Judicial

Las actuaciones que requieran autorización o control judicial deberán someterse a la autoridad judicial competente.

11. INDOTEL

Las medidas relacionadas con redes y servicios de telecomunicaciones deberán desarrollarse respetando las competencias del órgano regulador y la legislación aplicable.

12. Protección de datos

Los sistemas de información deberán adecuarse al marco vigente de protección de datos personales.

13. Evidencia digital

Las reglas administrativas de seguridad no podrán sustituir las normas procesales aplicables a la obtención y utilización de evidencia.

14. Contratación pública

Toda contratación deberá realizarse conforme al régimen jurídico vigente.

15. Derechos fundamentales

La aplicación del Sistema deberá interpretarse siempre de conformidad con los derechos fundamentales.

16. Principio de mínima intervención

Cuando existan varias medidas legalmente posibles, deberá preferirse aquella que alcance la finalidad de seguridad con menor afectación innecesaria de derechos.

17. Prohibición de tecnologías destructivas

RD Propone RD Propone

El Sistema no podrá incorporar como mecanismo ordinario de seguridad tecnologías destinadas deliberadamente a causar daños físicos a personas o destruir dispositivos mediante métodos que comprometan la integridad de las instalaciones o de sus usuarios.

18. Inteligencia artificial

La utilización de inteligencia artificial deberá permanecer subordinada a:

- Legalidad
- Supervisión humana
- Trazabilidad
- Protección de datos
- Auditoría
- Revisión de errores

19. Decisiones automatizadas

Una alerta automatizada no podrá constituir por sí sola fundamento suficiente para imponer una sanción.

20. Revisión periódica de la normativa

El marco deberá revisarse periódicamente para determinar si continúa respondiendo a los riesgos existentes.

CAPÍTULO XXXII
DISPOSICIONES TRANSITORIAS, FINALES Y PRINCIPIOS DE CIERRE

1. Diagnóstico inicial

Dentro del período que determine el reglamento de aplicación, el Ministerio de Justicia realizará un diagnóstico nacional de seguridad tecnológica y operacional penitenciaria.

2. Inventario nacional

Deberá elaborarse un inventario nacional de:

- Sistemas de comunicación
- Cámaras
- Controles de acceso
- Sistemas de detección
- Infraestructura eléctrica

RD Propone RD Propone

- Servidores
- Redes
- Equipos críticos
- Contratos
- Proveedores
- Capacidades del personal

3. Clasificación de riesgos

Los establecimientos serán clasificados según una metodología nacional uniforme.

4. Plan nacional

Con base en el diagnóstico se elaborará el Plan Nacional de Seguridad Penitenciaria Tecnológica e Integral.

5. Priorización

Los recursos deberán dirigirse inicialmente a los riesgos de mayor impacto.

6. Continuidad

Los sistemas existentes que sean funcionales podrán mantenerse mientras se integran progresivamente a la nueva arquitectura.

7. Migración

La sustitución de sistemas deberá realizarse mediante planes de migración que eviten interrupciones críticas.

8. Capacitación

Ningún sistema crítico deberá ser puesto en funcionamiento sin que el personal responsable haya recibido capacitación adecuada.

9. Certificación

Las funciones críticas deberán quedar sujetas al régimen nacional de certificación establecido en el capítulo correspondiente.

10. Auditoría inicial

Antes de declararse plenamente operativo el Sistema Nacional deberá realizarse una auditoría inicial.

RD Propone RD Propone

11. Evaluación anual

El Sistema deberá ser evaluado al menos una vez cada año.

12. Informe al Poder Ejecutivo

Los resultados deberán ser presentados a las autoridades superiores correspondientes.

13. Informe público

Deberá publicarse una versión pública del informe, preservando la información cuya divulgación pueda comprometer legítimamente la seguridad.

14. Revisión legislativa

El Congreso Nacional podrá evaluar periódicamente los resultados de la política y realizar las modificaciones legislativas que correspondan.

Artículo 32.15. Derogaciones

Quedan derogadas o modificadas únicamente aquellas disposiciones que resulten expresamente incompatibles con la presente ley, conforme al procedimiento legislativo correspondiente.

16. Reglamentación

El Poder Ejecutivo deberá dictar los reglamentos necesarios para la ejecución de la presente ley dentro del plazo establecido por la legislación.

17. Normas internas

Las instituciones deberán adaptar sus reglamentos, manuales y protocolos internos.

18. Contratos vigentes

Los contratos existentes deberán revisarse para determinar su compatibilidad con el nuevo Sistema, sin afectar derechos adquiridos ni desconocer obligaciones contractuales válidamente constituidas.

19. Sistemas tecnológicos existentes

La existencia de una tecnología anterior no obligará al Estado a sustituirla inmediatamente cuando pueda integrarse y continúe cumpliendo las condiciones de seguridad requeridas.

RD Propone RD Propone

20. Responsabilidad

La implementación deberá identificar claramente la responsabilidad de cada institución, dependencia, funcionario, proveedor y contratista.

21. Principio de continuidad

La seguridad penitenciaria constituye una función permanente del Estado. Los cambios de administración, autoridades o proveedores no deberán producir interrupciones injustificadas en los controles esenciales.

22. Principio de evaluación

Ningún componente del Sistema deberá considerarse definitivo.

Toda medida deberá poder ser evaluada, corregida, sustituida o eliminada cuando la evidencia demuestre que ha dejado de cumplir adecuadamente su finalidad.

23. Principio de proporcionalidad

La seguridad deberá alcanzarse mediante mecanismos proporcionales al riesgo.

24. Principio de humanidad

La modernización tecnológica del sistema penitenciario no podrá desconocer la dignidad de las personas privadas de libertad ni los derechos del personal, visitantes, abogados, familiares y demás personas autorizadas.

25. Principio de prevención

El Estado deberá privilegiar la prevención de incidentes sobre la reacción posterior.

26. Principio de inteligencia

La información deberá utilizarse para anticipar riesgos y no únicamente para documentar hechos después de ocurridos.

27. Principio de aprendizaje

Cada incidente deberá convertirse, cuando corresponda, en una oportunidad para mejorar procedimientos, tecnología, capacitación o infraestructura.

28. Principio de responsabilidad

La tecnología no elimina la responsabilidad humana.

RD Propone RD Propone

29. Principio de tecnología al servicio de la seguridad

La adquisición de tecnología deberá responder a necesidades institucionales previamente identificadas.

30. Principio de sostenibilidad

El Estado deberá priorizar soluciones que pueda mantener financieramente, técnicamente y operacionalmente.

31. Principio de interoperabilidad

Los componentes del Sistema deberán diseñarse para funcionar como una arquitectura integrada.

32. Principio de trazabilidad

Las actuaciones críticas deberán dejar evidencia suficiente para permitir su posterior revisión.

33. Principio de supervisión

Toda función crítica deberá estar sometida a controles y auditorías.

34. Principio de protección

La finalidad última del Sistema será proteger:

- La vida
- La integridad
- La seguridad
- Los derechos
- La administración penitenciaria
- La sociedad

35. Principio nacional de cierre

La República Dominicana establecerá un sistema penitenciario en el cual la seguridad no dependa de una sola tecnología, una sola institución, una sola persona o un solo procedimiento.

La seguridad deberá resultar de la combinación de:

- Prevención

RD Propone RD Propone

- Control
- Tecnología
- Inteligencia
- Personal capacitado
- Comunicación legítima
- Infraestructura
- Investigación
- Responsabilidad
- Auditoría
- Evaluación permanente

36. Fórmula integral del Sistema

El Sistema Nacional de Seguridad Penitenciaria deberá funcionar bajo la siguiente secuencia:

PREVENIR – CONTROLAR – DETECTAR – LOCALIZAR – ALERTAR – RESPONDER – PRESERVAR – INVESTIGAR - SANCIONAR CUANDO – CORRESPONDA – CORREGIR – AUDITAR – APRENDER - VOLVER A PREVENIR.

37. Objetivo final

La política nacional tendrá como objetivo reducir progresivamente la capacidad de las estructuras criminales para utilizar establecimientos penitenciarios como plataformas de coordinación ilícita, sin convertir el sistema penitenciario en un espacio ajeno al Estado de derecho.

RD Propone RD Propone