

PROYECTO DE REGLAMENTO DE APLICACIÓN DEL SISTEMA NACIONAL DE SEGURIDAD PENITENCIARIA INTEGRAL, TECNOLÓGICA Y DE COMUNICACIONES

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1.- Objeto. El presente Reglamento establece las normas de aplicación, procedimientos generales y estándares mínimos para ejecutar la Ley sobre Seguridad Penitenciaria Integral, Tecnológica y de Comunicaciones.

Artículo 2.- Ámbito. Se aplica a los establecimientos, dependencias y servicios penitenciarios y correccionales sometidos al régimen de la ley, así como al personal, contratistas, proveedores, visitantes y terceros en cuanto corresponda.

Artículo 3.- Principios. La aplicación observará legalidad, dignidad humana, necesidad, proporcionalidad, prevención, trazabilidad, confidencialidad, protección de datos, seguridad de la información, continuidad, neutralidad tecnológica y rendición de cuentas.

Artículo 4.- Jerarquía normativa. En caso de conflicto, prevalecerán la Constitución, las leyes y las decisiones judiciales sobre este Reglamento, protocolos o manuales.

Artículo 5.- Normas técnicas. Los estándares técnicos podrán actualizarse sin modificar el Reglamento cuando no alteren derechos, competencias ni obligaciones esenciales establecidas por la ley.

TÍTULO II

GOBERNANZA Y ORGANIZACIÓN DEL SISTEMA

Artículo 6.- Dirección y coordinación. El Ministerio de Justicia ejercerá las funciones de rectoría, coordinación y dirección administrativa que le atribuya el ordenamiento vigente.

Artículo 7.- Dirección General de Servicios Penitenciarios y Correccionales. La DGSPC ejecutará las funciones operacionales que le correspondan como organismo adscrito al Ministerio de Justicia y actuará conforme a la legislación vigente.

Artículo 8.- Coordinación con el Ministerio Público. La coordinación con el Ministerio Público se realizará dentro de las competencias constitucionales y legales de ambas instituciones, especialmente cuando un incidente pueda tener relevancia penal.

Artículo 9.- Coordinación tecnológica. La estructura especializada del Ministerio de Justicia coordinará los componentes tecnológicos del sistema sin sustituir a las autoridades de investigación, persecución penal, regulación de telecomunicaciones o control judicial.

Artículo 10.- Centro Nacional de Monitoreo. Funcionará como centro técnico de supervisión, correlación de alertas, análisis y apoyo a la gestión de incidentes. Sus operadores no podrán adoptar decisiones reservadas por ley a otras autoridades.

Artículo 11.- Responsables locales. Cada establecimiento designará responsables de seguridad tecnológica y de gestión de incidentes, con funciones, suplencias y niveles de acceso definidos.

Artículo 12.- Matriz de responsabilidades. El Ministerio de Justicia aprobará una matriz nacional que determine quién previene, detecta, valida, responde, investiga, preserva evidencia, audita y corrige.

TÍTULO III

GESTIÓN DE RIESGOS Y CLASIFICACIÓN DE ESTABLECIMIENTOS

Artículo 13.- Evaluación nacional de riesgos. Cada establecimiento será evaluado mediante una metodología uniforme que considere población, infraestructura, incidentes, personal, proveedores, accesos, comunicaciones, tecnología y vulnerabilidades.

Artículo 14.- Categorías de riesgo. Los establecimientos se clasificarán en categorías de riesgo que determinarán la intensidad mínima de los controles.

Artículo 15.- Actualización. La clasificación se revisará periódicamente y después de incidentes graves, cambios de infraestructura o alteraciones relevantes del riesgo.

Artículo 16.- Plan de tratamiento. Cada establecimiento contará con un plan de tratamiento de riesgos con responsables, plazos, recursos, indicadores y medidas correctivas.

TÍTULO IV

PREVENCIÓN Y CONTROL DE DISPOSITIVOS NO AUTORIZADOS

Artículo 17.- Política de dispositivos. Cada establecimiento tendrá una política escrita sobre dispositivos permitidos, restringidos y prohibidos, diferenciando las necesidades de personal, proveedores, visitantes y personas privadas de libertad.

Artículo 18.- Autorización de equipos. Los equipos institucionales autorizados deberán estar identificados y registrados. Los equipos personales solo podrán ingresar cuando exista autorización expresa y justificación funcional.

Artículo 19.- Ingreso de personas. Los controles de ingreso se diseñarán según riesgo e incluirán identificación, inspección autorizada, control de objetos y registro de incidencias.

Artículo 20.- Vehículos y suministros. Los vehículos, paquetes, herramientas, alimentos, equipos y suministros estarán sujetos a controles de ingreso, inventario y salida conforme a su nivel de riesgo.

Artículo 21.- Detección tecnológica. Podrán emplearse sistemas de detección y localización técnicamente homologados, con pruebas periódicas y registro de disponibilidad.

Artículo 22.- Verificación de alertas. Toda alerta relevante deberá ser validada por personal autorizado antes de generar actuaciones sancionadoras o investigaciones, sin perjuicio de las medidas urgentes de protección.

Artículo 23.- Localización. La localización técnica tendrá como finalidad apoyar la identificación del área de riesgo y orientar la respuesta institucional, sin presumir por sí misma la responsabilidad de una persona.

Artículo 24.- Intercepción. Ningún equipo instalado en virtud de este Reglamento autoriza por sí mismo la interceptación o acceso al contenido de comunicaciones privadas.

Artículo 25.- Tecnologías destructivas. Se prohíbe utilizar sistemas eléctricos, electromagnéticos o de otro tipo con finalidad de destruir o deteriorar dispositivos cuando ello pueda afectar personas, infraestructura o servicios. La energía e infraestructura podrán utilizarse para seguridad, monitoreo y continuidad.

Artículo 26.- Pruebas de penetración. Se realizarán pruebas controladas y documentadas de los controles, sin poner en riesgo innecesario a personas ni instalaciones.

Artículo 27.- Vulnerabilidades. Toda vulnerabilidad identificada deberá incorporarse a un registro, asignarse a un responsable y contar con fecha objetivo de corrección.

TÍTULO V

COMUNICACIONES LEGÍTIMAS Y SERVICIOS TECNOLÓGICOS

Artículo 28.- Sistema de comunicaciones institucionales. La administración habilitará, según disponibilidad y condiciones de seguridad, medios institucionales de comunicación para atender necesidades legítimas.

Artículo 29.- Identificación de usuarios. Los usuarios de servicios institucionales deberán ser identificados conforme a procedimientos de autenticación y registro.

Artículo 30.- Videocomunicación. Las videocomunicaciones podrán habilitarse mediante plataformas institucionales controladas y con medidas de seguridad.

Artículo 31.- Comunicaciones jurídicas y consulares. Los controles deberán respetar las garantías especiales establecidas para comunicaciones con abogados, defensores, autoridades consulares y otros sujetos protegidos por ley.

Artículo 32.- Digitalización para reinserción. Podrán habilitarse servicios digitales educativos, administrativos y de reinserción en ambientes controlados.

Artículo 33.- Registro de uso. Los registros de utilización deberán limitarse a los datos necesarios para seguridad, facturación, auditoría o administración, según corresponda.

TÍTULO VI

MONITOREO, INFORMACIÓN, INTELIGENCIA Y EVIDENCIA

Artículo 34.- Registro nacional de incidentes. Se establecerá un registro nacional con identificador único para incidentes de seguridad tecnológica y de comunicaciones.

Artículo 35.- Integración. Los sistemas podrán integrar, según base jurídica y finalidad, información de accesos, CCTV, alertas, inventarios, mantenimiento y eventos.

Artículo 36.- Control de acceso a información. El acceso será por roles y bajo el principio de necesidad de conocer.

Artículo 37.- Inteligencia. Los análisis deberán distinguir información operativa, inteligencia y evidencia, evitando utilizar una categoría como sustituta de otra.

Artículo 38.- Evidencia digital. La evidencia digital será preservada conforme a protocolos de integridad, autenticidad, trazabilidad y cadena de custodia.

Artículo 39.- Dispositivos incautados. Los dispositivos incautados serán embalados, identificados, registrados y puestos a disposición de la autoridad competente cuando proceda.

Artículo 40.- Contenido protegido. No se accederá al contenido de dispositivos o comunicaciones protegidas sin la habilitación legal correspondiente.

Artículo 41.- Inteligencia artificial. Las herramientas automatizadas podrán apoyar la detección de anomalías, análisis de patrones y priorización de alertas, pero deberán contar con supervisión humana y mecanismos de auditoría.

Artículo 42.- Registro de decisiones automatizadas. Los sistemas que generen alertas de alto impacto deberán conservar información suficiente para reconstruir su funcionamiento y permitir revisión.

TÍTULO VII

CONTROL DE ACCESO, MOVILIDAD, BIENES E INFRAESTRUCTURA

Artículo 43.- Zonificación. Los establecimientos establecerán zonas públicas, controladas, restringidas y críticas, con niveles diferenciados de autorización.

Artículo 44.- Credenciales. Las credenciales serán individuales, temporales cuando corresponda, y deberán poder ser anuladas inmediatamente ante pérdida, terminación de funciones o riesgo.

Artículo 45.- Visitantes. Los visitantes deberán cumplir los controles establecidos, preservando las garantías especiales aplicables.

Artículo 46.- Proveedores. Los proveedores deberán contar con autorización, identificación, orden de trabajo y supervisión proporcional al riesgo.

Artículo 47.- Doble control. Las operaciones de alto riesgo podrán requerir dos funcionarios autorizados o mecanismos equivalentes de control.

Artículo 48.- Bienes y paquetes. El ingreso y salida de bienes estará sujeto a registro y reconciliación.

Artículo 49.- Infraestructura crítica. Los centros de datos, telecomunicaciones, electricidad, CCTV, control de acceso y sistemas de respaldo tendrán controles reforzados.

Artículo 50.- Mantenimiento. Todo mantenimiento en infraestructura crítica deberá generar orden de trabajo, identificación del técnico, horario, alcance y cierre documentado.

TÍTULO VIII

PERSONAL, INTEGRIDAD, CAPACITACIÓN Y TERCEROS

Artículo 51.- Perfiles. Los puestos críticos tendrán perfiles de competencia definidos.

Artículo 52.- Capacitación. El personal recibirá formación inicial, especializada y continua.

Artículo 53.- Certificación. Las funciones críticas podrán requerir certificación y recertificación.

Artículo 54.- Integridad. Se establecerán controles para prevenir corrupción, complicidad, conflictos de interés y manipulación de sistemas.

Artículo 55.- Canales de reporte. Existirán canales seguros para reportar irregularidades.

Artículo 56.- Terceros. Los contratistas y proveedores deberán cumplir programas de seguridad y confidencialidad compatibles con sus funciones.

Artículo 57.- Acceso de proveedores tecnológicos. El acceso remoto será excepcional, autorizado, limitado, registrado y revocable.

TÍTULO IX

RESPUESTA A INCIDENTES

Artículo 58.- Ciclo de respuesta. La gestión seguirá las etapas de alerta, validación, control, preservación, intervención, documentación, escalamiento, investigación, corrección y cierre.

Artículo 59.- Niveles de severidad. El protocolo nacional establecerá niveles de severidad y tiempos objetivo de respuesta.

Artículo 60.- Seguridad de personas. La protección de la vida e integridad tendrá prioridad.

Artículo 61.- Preservación. Los sistemas deberán preservar imágenes, registros y demás información relevante conforme a la ley.

Artículo 62.- Escalamiento. Los incidentes serán comunicados al nivel institucional correspondiente y, cuando proceda, al Ministerio Público u otra autoridad competente.

Artículo 63.- Análisis de causa raíz. Los incidentes graves deberán generar un análisis de causa raíz y un plan de corrección.

Artículo 64.- Cierre. Un incidente solo se considerará cerrado cuando se hayan documentado acciones, responsables, evidencias, medidas correctivas y lecciones aprendidas.

TÍTULO X

CIBERSEGURIDAD, DATOS Y CONTINUIDAD

Artículo 65.- Inventario tecnológico. Cada establecimiento mantendrá un inventario actualizado de activos tecnológicos críticos.

Artículo 66.- Identidades. Las cuentas de usuarios serán individuales y sujetas a controles de privilegios.

Artículo 67.- Autenticación reforzada. Los sistemas críticos utilizarán mecanismos reforzados de autenticación cuando técnicamente corresponda.

Artículo 68.- Segmentación. Los sistemas críticos deberán segmentarse para reducir la propagación de incidentes.

Artículo 69.- Actualizaciones. Se implementará gestión documentada de actualizaciones y vulnerabilidades.

Artículo 70.- Copias de seguridad. Los sistemas críticos contarán con respaldos periódicos y pruebas de recuperación.

Artículo 71.- Protección de datos. El tratamiento de datos se ajustará a la legislación vigente y a las políticas institucionales de seguridad.

Artículo 72.- Continuidad. Cada establecimiento tendrá un plan de continuidad y recuperación de servicios críticos.

Artículo 73.- Pruebas. Los planes de continuidad serán sometidos a pruebas periódicas.

TÍTULO XI

TECNOLOGÍA, CONTRATACIÓN, AUDITORÍA Y SOSTENIBILIDAD

Artículo 74.- Estudios previos. Antes de adquirir tecnología crítica deberá documentarse la necesidad, alternativas, riesgos, costos de ciclo de vida y requisitos de interoperabilidad.

Artículo 75.- Contratación. Los procesos se sujetarán a la Ley 47-25, el Decreto 52-26 y las disposiciones emitidas por la DGCP que resulten aplicables.

Artículo 76.- Homologación. Los sistemas críticos deberán superar pruebas técnicas antes de su aceptación.

Artículo 77.- Criterios de aceptación. Los contratos definirán indicadores de desempeño, disponibilidad, seguridad, tiempos de respuesta y mantenimiento.

Artículo 78.- Dependencia tecnológica. Los contratos deberán reducir riesgos de dependencia mediante documentación, portabilidad, capacitación y condiciones de salida razonables.

Artículo 79.- Auditoría. Las tecnologías críticas estarán sujetas a auditorías funcionales, de seguridad y de cumplimiento.

Artículo 80.- Costos. La evaluación económica considerará adquisición, instalación, licencias, conectividad, mantenimiento, actualización, capacitación, reposición y retiro.

Artículo 81.- Proveedores. Se evaluará el desempeño de proveedores y se documentarán incumplimientos y medidas correctivas.

TÍTULO XII

INDICADORES, TRANSPARENCIA, IMPLEMENTACIÓN Y DISPOSICIONES FINALES

Artículo 82.- Indicadores. El sistema utilizará indicadores de prevención, detección, respuesta, reincidencia, disponibilidad, mantenimiento, capacitación, costos y resultados.

Artículo 83.- Tablero nacional. El Ministerio de Justicia dispondrá de un tablero de seguimiento con niveles de acceso diferenciados.

Artículo 84.- Información pública. Se publicará información agregada que permita rendición de cuentas sin revelar información cuya reserva sea legalmente necesaria.

Artículo 85.- Plan de implementación. La ejecución se realizará progresivamente conforme a diagnóstico, priorización de riesgo, pilotos, evaluación y expansión.

Artículo 86.- Fase inicial. La primera fase comprenderá diagnóstico nacional, inventario, evaluación de vulnerabilidades y medidas inmediatas de contención.

Artículo 87.- Pilotos. Los pilotos deberán contar con objetivos, indicadores, presupuesto, responsables y criterios de continuación o corrección.

Artículo 88.- Expansión. La expansión nacional dependerá de resultados documentados, disponibilidad presupuestaria, capacidad de mantenimiento y cumplimiento de estándares.

Artículo 89.- Evaluación anual. El sistema será evaluado anualmente y los resultados servirán para actualizar prioridades.

Artículo 90.- Revisión del Reglamento. El Reglamento será revisado cuando cambios legislativos, tecnológicos o institucionales lo hagan necesario.

Artículo 91.- Protocolos técnicos. El Ministerio de Justicia aprobará los protocolos y manuales técnicos necesarios, respetando la ley y este Reglamento.

Artículo 92.- Transición. Los establecimientos contarán con un período de adecuación definido en el plan nacional.

Artículo 93.- Sistemas existentes. Las tecnologías existentes serán evaluadas antes de su sustitución o ampliación.

Artículo 94.- Continuidad. La implementación no podrá interrumpir servicios penitenciarios esenciales.

Artículo 95.- Responsabilidad. Los responsables de cada proceso deberán documentar sus actuaciones y cumplir los controles de auditoría.

Artículo 96.- Entrada en vigor. El presente Reglamento entrará en vigor conforme al decreto que lo apruebe.

Artículo 97.- Cláusula final. Las disposiciones de este Reglamento deberán interpretarse y aplicarse de manera compatible con la Constitución, las leyes y las decisiones judiciales aplicables.