PODER EJECUTIVO

SECRETARIA DE SEGURIDAD Y PROTECCION CIUDADANA

ANEXO 1 del Acuerdo 09/XLVII/21 del Consejo Nacional de Seguridad Pública, aprobado en su Cuadragésima Séptima Sesión Ordinaria, celebrada el 16 de diciembre de 2021, publicado el 29 de diciembre de 2021.

Al margen un logotipo, que dice: Secretaría de Seguridad y Protección Ciudadana (SSPC).- Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP).- Centro Nacional de Información (CNI).

Nuevos Lineamientos del Registro Nacional de Detenciones (RND).

JESÚS DAVID PÉREZ ESPARZA, Titular del Centro Nacional de Información (CNI) del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), con fundamento en lo dispuesto por los artículos 16, párrafo quinto, y 21, párrafos noveno y décimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 2, 3, 4, 5, fracciones II, VIII y XVII, 6, 7, fracciones I, IX y XVI, 10, fracción VII, 17, 19, fracciones I, II y III, 39, Apartado A, fracciones I, IV y V, y Apartado B, fracciones V y XV, 77, fracciones IV y VI, 109, 110, 112, 117, y 118 de la Ley General del Sistema Nacional de Seguridad Pública; 3, 4 y 12 de la Ley Nacional del Registro de Detenciones; 147 y 150 del Código Nacional de Procedimientos Penales; y 1, 4, 6, fracción III, 10, 11, fracciones II y XVII, y 12, fracciones VI, X, XX, XXII y XXIV del Reglamento del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, y

CONSIDERANDO

Que el artículo 21, párrafos noveno y décimo, de la Constitución Política de los Estados Unidos Mexicanos, dispone que la seguridad pública es una función del Estado a cargo de la federación, las entidades federativas y los municipios; la cual comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en la Constitución;

Que el artículo 21 constitucional establece también que, para lograr dicho fin, las instituciones de seguridad pública, incluyendo la Guardia Nacional, serán de carácter civil, disciplinado y profesional. El ministerio público y las instituciones policiales de los tres órdenes de gobierno deberán coordinarse entre sí para cumplir los fines de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública;

Que el artículo 16, párrafo quinto, de la Constitución Política de los Estados Unidos Mexicanos, establece la obligación de que exista un registro inmediato de la detención de todas las personas en el territorio nacional, y que éste representa uno de los derechos humanos más importantes en México;

Que el artículo 2 de la Ley General del Sistema Nacional de Seguridad Pública (LGSNSP), establece que la seguridad pública tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos;

Que de conformidad con el artículo 4 de la LGSNSP, el Sistema Nacional de Seguridad Pública cuenta para su funcionamiento y operación con las instancias, instrumentos, políticas, acciones y servicios previstos en la misma;

Que en términos de lo dispuesto por el artículo 17 y 19 de la LGSNSP, el SESNSP es el órgano operativo del Sistema Nacional de Seguridad Pública que goza de autonomía técnica, de gestión y presupuestal, y cuenta dentro de su estructura con el Centro Nacional de Información (CNI), quien es el responsable de regular el Sistema Nacional de Información en Seguridad Pública (SNI);

Que según lo dispuesto por los artículos previamente referidos, el Sistema Nacional de Información en Seguridad Pública está conformado por un conjunto de bases de datos que contienen información en materia de detenciones, vehículos, armamento, equipo y personal de seguridad pública, medidas cautelares, soluciones alternas y formas de terminación anticipada, así como criminalística, huellas dactilares, teléfonos celulares, personas sentenciadas y servicios de seguridad privada;

Que la Estrategia Nacional de Seguridad Pública del Gobierno de la República, publicada en el Diario Oficial de la Federación el 16 de mayo de 2019, establece como uno de sus objetivos el Pleno respeto y promoción de los Derechos Humanos. Como tal, el Gobierno de México se compromete a erradicar la represión y garantizar, con todos los métodos posibles, que ninguna persona será torturada, desaparecida o asesinada por un cuerpo de seguridad del Estado; y que, de ocurrir, el Estado mexicano, en su conjunto, se compromete a investigar, sancionar y erradicar esta práctica;

Que en un sentido similar, dicha Estrategia Nacional establece como parte del objetivo de Regeneración ética de la sociedad, que es vital el ejercicio de un gobierno austero, honesto, transparente, incluyente, respetuoso de las libertades; apegado a los derechos y sensible a las necesidades de los más débiles y vulnerables;

Que de conformidad con el artículo 112 de la LGSNSP, el Registro Nacional de Detenciones (RND) forma parte del Sistema Nacional de Información en Seguridad Pública. Por ello, su diseño, planeación, uso, explotación de datos, publicidad y en su caso, reforma operativa y de gestión, será una función prioritaria y estratégica a cargo del C. Titular del Centro Nacional de Información (CNI) y del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), en los términos previstos por la ley de la materia;

Que la Ley Nacional del Registro de Detenciones, aprobada y publicada en el Diario Oficial de la Federación el 27 de mayo de 2019, tiene como objetivo prevenir la violación de los derechos humanos de la persona detenida; así como cualquier acto de tortura, tratos crueles, inhumanos y degradantes, o la desaparición forzada;

Que el artículo 3 de la Ley Nacional del Registro de Detenciones, establece que el Registro Nacional de Detenciones consiste en una base de datos que concentra la información a nivel nacional sobre las personas detenidas, conforme a las facultades de las autoridades durante las etapas del proceso penal o del procedimiento administrativo sancionador;

Que el artículo 5 de la Ley Nacional del Registro de Detenciones estipula que el Registro Nacional de Detenciones deberá contar con un Sistema de Consulta que permita a las personas, a través de herramientas tecnológicas, tener acceso a una versión pública de la información de las detenciones practicadas a lo largo y ancho de todo el país, sin importar el lugar en que éstas ocurrieron;

Que la Ley Nacional del Registro de Detenciones establece también que será el Centro Nacional de Información (CNI), el órgano encargado de emitir las disposiciones, protocolos, mecanismos y reglas de operación, y que, además, deberá darlos a conocer a todas las personas, garantizando el derecho a la información, bajo los principios de transparencia, igualdad, equidad y máxima publicidad;

Que con base en lo dispuesto por los artículos 147 y 150 del Código Nacional de Procedimientos Penales, los integrantes de las instituciones policiales que realicen o ejecuten una detención deberán realizar el registro de la misma;

Que el artículo 12 del Reglamento del SESNSP, establece que el Centro Nacional de Información (CNI) vigila el cumplimiento de los criterios y niveles de acceso a los que se sujetarán el suministro, intercambio, la consulta y actualización de la información contenida en las bases de datos del Sistema Nacional de Información en Seguridad Pública (SNI);

Que de acuerdo con el artículo 19 de la LGSNSP y el artículo 12 del Reglamento del SESNSP el CNI es el órgano responsable del diseño, implementación, despliegue, monitoreo y evaluación de otros mecanismos elementales de justicia, complementarios al Registro Nacional de Detenciones (RND), entre los que se encuentran: (a) la coordinación de la Línea Única de Emergencias 9-1-1, (b) la publicación de la incidencia delictiva oficial del Estado mexicano en coordinación con las 32 instancias de procuración de justicia de las entidades federativas y la Fiscalía General de la República (FGR), (c) la gestión de los sistemas de video-vigilancia (SVV), (d) la coordinación con todos los Centros de Atención de Llamadas de Emergencia (CALLE), (e) la coordinación con los Complejos de Seguridad, también conocidos como C4 o C5, (f) el diseño e implementación del Informe Policial Homologado (IPH), (g) el despliegue de las redes de radiocomunicación policial y sus pares satelitales, de fibra óptica u otros que cumplan dicha función, (h) la gestión integral de la línea única de denuncia anónima 0-89, e, (i) el diseño de la regulación de todos los Registros y Bases de Datos Nacionales;

Que el Registro Nacional de Detenciones (RND) se encuentra entre las políticas más importantes en materia de protección a los derechos humanos en el país, y por ende, es una de las prioridades más altas del Gobierno de México;

Que los Lineamientos para el adecuado uso del Registro Nacional de Detenciones (RND) y sus eventuales modificaciones, deben ser obligatorios, aplicados y observados por todas las instituciones de seguridad pública de los tres órdenes de gobierno. Por lo que su conocimiento general es necesario a través de los canales oficiales con los que cuenta el Estado mexicano;

Que con fecha de 16 de diciembre de 2021, el Consejo Nacional de Seguridad Pública (CNSP), a través del Acuerdo 09/XLVII/21, aprobó e instruyó la publicación de los presentes Lineamientos para el Funcionamiento, Operación y Conservación del Registro Nacional de Detenciones (RND); y,

Que en cumplimiento de lo anterior, y con fundamento en lo establecido por el artículo 12 de la Ley Nacional de Registro de Detenciones, he tenido a bien expedir los siguientes:

LINEAMIENTOS PARA EL FUNCIONAMIENTO, OPERACIÓN Y CONSERVACIÓN DEL REGISTRO NACIONAL DE DETENCIONES (RND)

PRIMERO. OBJETO.

Los presentes Lineamientos tienen por objeto regular la integración, operación, conservación y funcionamiento del Registro Nacional de Detenciones (RND), además de establecer los procedimientos que garanticen el control y seguimiento de la detención de todas las personas por parte de la autoridad.

El RND tiene la finalidad de prevenir la violación de los derechos humanos de la persona detenida, actos de tortura, tratos crueles, inhumanos y degradantes o la desaparición forzada. Su objetivo principal es informar el lugar donde se encuentra la persona detenida.

SEGUNDO. ÁMBITO DE APLICACIÓN.

Los presentes Lineamientos son de observancia obligatoria y aplicación general para:

I. La Secretaría de Seguridad y Protección Ciudadana (SSPC);

II. El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP);

III. La Guardia Nacional;

IV. La Fuerza Armada permanente que realice funciones de Seguridad Pública;

V. Las Secretarías de Seguridad Pública, Secretarías de Seguridad Ciudadana o sus equivalentes en cada entidad federativa; las Secretarías de Seguridad Pública Municipal, Direcciones de Seguridad Pública Municipal o sus equivalentes en los municipios de cada entidad federativa;

VI. La Fiscalía General de la República (FGR);

VII. Las Procuradurías o Fiscalías Generales de Justicia de las entidades federativas;

VIII. El Órgano Administrativo Desconcentrado Prevención y Readaptación Social (OADPYRS);

IX. Las Subsecretarías del Sistema Penitenciario o sus equivalentes en cada entidad federativa;

X. Los Jueces Municipales, Cívicos, Calificadores, Conciliadores o cualquier otra autoridad que, en funciones de seguridad pública, tomen conocimiento de hechos que puedan ser constitutivos de infracciones administrativas en el ámbito de la justicia cívica; y,

XI. En general, todas las dependencias encargadas de la seguridad pública, justicia cívica, procuración de justicia, y sistema penitenciario, o aquellas que realicen funciones similares.

La aplicación de los presentes Lineamientos comprende, desde la detención de una persona por un hecho probablemente delictivo o una infracción administrativa, hasta su liberación o ingreso al sistema penitenciario, centro de detención preventiva municipal o similares.

Una vez ingresada la información de la persona detenida, el sistema generará automáticamente el número de registro de la detención. Dicho número debe constar en el Informe Policial Homologado (IPH) y servirá para todas las actualizaciones que se realicen en el Registro Nacional de Detenciones.

En caso de que la persona detenida ingrese al sistema penitenciario, la autoridad que corresponda estará obligada a actualizar el Registro Nacional de Detenciones de forma inmediata y con base en el número de origen. La actualización deberá vincularse con el Registro Nacional de Información Penitenciaria (RNIP) a cargo de las autoridades penitenciarias. En seguimiento al principio constitucional de presunción de inocencia, la información contenida en el Registro Nacional de Detenciones no será considerada un antecedente penal.

TERCERO. GLOSARIO DE TÉRMINOS.

Para los efectos de los presentes Lineamientos, se entiende por:

I. **Autoridad administrativa:** Los Jueces Municipales, Cívicos, Calificadores, Conciliadores o cualquier otra autoridad competente para conocer y sancionar las infracciones administrativas en el ámbito de la justicia cívica.

II. **Base de datos:** El subconjunto sistematizado de la información que forma parte del Registro Nacional de Detenciones (RND).

III. **Centro de detención preventiva municipal o similares:** Es la institución donde se interna a las personas que se encuentran cumpliendo una sanción de carácter administrativo o a disposición de alguna autoridad, en espera de que se resuelva su situación jurídica. La sanción administrativa no podrá exceder del plazo de 36 horas, según lo dispuesto por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

IV. **Centro penitenciario:** Espacio físico destinado para el cumplimiento de la prisión preventiva, así como para la ejecución de penas que ameritan la privación de la libertad.

V. **CNI:** El Centro Nacional de Información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.

VI. **CNSP:** El Consejo Nacional de Seguridad Pública.

VII. **Conferencias Nacionales:** Son las cuatro Conferencias a las que se refiere la LGSNSP relativas a: (a) las instituciones de procuración de justicia, (b) las secretarías de seguridad pública de las entidades federativas, (c) los órganos estatales del sistema penitenciario y (e) las secretarías de seguridad pública municipal o equivalentes.

VIII. **CUIP:** Clave Única de Identificación Policial.

IX. **Derechos ARCO:** Acceso, Rectificación, Cancelación y Oposición.

X. **Falta administrativa:** Cualquier infracción a un reglamento municipal o estatal en el ámbito de su competencia.

XI. **Instituciones de seguridad pública:** Las instituciones policiales, de procuración de justicia, del sistema penitenciario y dependencias encargadas de las tareas de seguridad pública en la federación, las entidades federativas y los municipios, de conformidad con el artículo 5 fracción VIII de la LGSNSP; así como las competentes para conocer y sancionar las infracciones administrativas.

XII. **Instituciones policiales:** Los cuerpos de policía, de vigilancia y custodia de los establecimientos penitenciarios, de detención preventiva, o de centros de arraigo; y en general, todas las dependencias encargadas de la seguridad pública a nivel federal, estatal y municipal, que realicen funciones similares, incluyendo a la Fuerza Armada permanente que realice tareas de seguridad pública, de conformidad con el artículo 5 fracción X de la LGSNSP.

XIII. **Instituciones de procuración de justicia:** Las instituciones de la federación y de las entidades federativas que integran al ministerio público, los servicios periciales, las policías de investigación y demás auxiliares de aquél, de conformidad con el artículo 5 fracción IX de la LGSNSP.

XIV. **Informe Policial Homologado (IPH):** El Informe Policial Homologado de hechos probablemente delictivos o de infracciones administrativas, mismo que puede ser impreso o electrónico. La última versión al momento de la publicación de este documento se refiere a la actualización llevada a cabo en 2019.

XV. **Justicia Cívica:** Se refiere al componente del Modelo Nacional de Policía y Justicia Cívica (MNPyJC) elaborado por el SESNSP, que busca la solución institucional de los conflictos vecinales o comunitarios, a través de la intervención oportuna de las autoridades locales. Esto se logra por medio de audiencias públicas, abiertas, contradictorias y orales.

XVI. **Ley:** La Ley Nacional del Registro de Detenciones.

XVII. **Ley General:** La Ley General del Sistema Nacional de Seguridad Pública (LGSNSP).

XVIII. **Lineamientos:** Los Lineamientos para el funcionamiento, operación y conservación del Registro Nacional de Detenciones (RND).

XIX. **Número de registro de la detención:** El número asignado automáticamente por el sistema, que tiene como finalidad establecer el seguimiento y trazabilidad de la persona detenida, hasta su liberación o ingreso al sistema penitenciario o, en su caso, al centro de detención preventiva municipal o similares.

XX. **Persona detenida:** La persona privada de la libertad por parte de una autoridad integrante de alguna de las instituciones de seguridad pública; por cualquiera de los siguientes supuestos: (a) detención en flagrancia, (b) orden de aprehensión, (c) caso urgente, (d) retención ministerial, (e) prisión preventiva, y (f) orden de detención con fines de extradición pasiva, reclusión, arraigo, reaprehensión o arresto administrativo.

XXI. **Plataforma o Sistema Informático:** El sistema de gestión electrónico y virtual, a través de internet, diseñado por la Secretaría en conjunto con el CNI, mediante el cual los usuarios del RND realizan la primera, segunda y/o tercera captura de los datos de la persona detenida.

XXII. **RND:** El Registro Nacional de Detenciones es la base de datos que concentra la información a nivel nacional sobre todas las personas detenidas en territorio nacional, conforme a las facultades de las autoridades competentes, durante las etapas del procedimiento penal o administrativo sancionador correspondiente. Este Registro forma parte del Sistema Nacional de Información.

XXIII. **RNIP:** El Registro Nacional de Información Penitenciaria. Este Registro forma parte del Sistema Nacional de Información.

XXIV. **RNPSP:** El Registro Nacional de Personal de Seguridad Pública. Este Registro forma parte del Sistema Nacional de Información.

XXV. **SAU:** Sistema de Administración de Usuarios.

XXVI. **Secretaría:** La Secretaría de Seguridad y Protección Ciudadana (SSPC).

XXVII. **Servicio de interoperabilidad bidireccional:** La capacidad de un sistema para lograr la intercomunicación con otro sistema en un lenguaje interoperable y compatible entre ellos.

XXVIII. **SESNSP:** El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.

XXIX. **Sistema de Consulta:** El Sistema de Consulta del Registro Nacional de Detenciones que permite a cualquier persona realizar una búsqueda electrónica en internet sobre personas detenidas, al que se refiere el artículo 31 de la Ley.

XXX. **SNI:** El Sistema Nacional de Información en Seguridad Pública, al que se refiere el artículo 5 fracción XVII de la Ley General.

XXXI. **SNSP:** El Sistema Nacional de Seguridad Pública según se regula en la Ley General.

XXXII. **Sujeto Obligado:** Persona servidora pública que por motivo de su empleo, encargo o comisión intervenga en la captura, ingreso, envío, recepción, manejo, consulta o actualización de la información que integra el RND.

CUARTO. ALCANCE.

Los presentes Lineamientos regulan el funcionamiento, operación y conservación del RND. Con ello, se busca proteger los derechos humanos de las personas detenidas, con absoluto respeto a su dignidad, evitando toda discriminación motivada por origen étnico o nacional, género, edad, discapacidad, condición social, condición de salud, religión, opiniones, preferencias sexuales, estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

Asimismo, estos Lineamientos reglamentan la administración, resguardo e implementación del Sistema de Consulta que permite ubicar a las personas detenidas a través de su sitio web.

Estos Lineamientos también contemplan la conservación del RND. Dicha actividad será responsabilidad de la Secretaría, misma que deberá tomar todas las medidas pertinentes para la disponibilidad, cuidado y resguardo de la información contenida en dicha base de datos.

QUINTO. CUMPLIMIENTO.

Las instituciones de seguridad pública de los tres órdenes de gobierno deberán asegurar el estricto cumplimiento de los presentes Lineamientos. Asimismo, dichas instituciones están obligadas, en todo momento, a implementar las acciones de carácter técnico, jurídico y administrativo que resulten necesarias para el adecuado funcionamiento, operación, consulta y explotación del RND.

La Secretaría será la encargada de asegurar la administración, operación y disponibilidad del sistema informático necesario para el funcionamiento del RND y su Sistema de Consulta.

SEXTO. IMPLEMENTACIÓN DEL RND.

La implementación del RND estará a cargo de la Secretaría, el SESNSP y las instituciones de seguridad pública de los tres órdenes de gobierno, en el ámbito de sus respectivas competencias.

Cada una de las instituciones señaladas en el párrafo anterior, deberán realizar las acciones correspondientes para la operación y disponibilidad del sistema informático, a fin de realizar la captura, ingreso, envío, recepción, manejo, actualización, interconexión, consulta y explotación del RND. Asimismo, estas instituciones de los tres órdenes de gobierno deberán llevar a cabo todas aquellas adecuaciones necesarias a su normatividad interna, para asegurar el cabal cumplimiento del RND y, en su caso, establecer las sanciones correspondientes.

Los sujetos obligados de las instituciones de seguridad pública tomarán las acciones necesarias para que la información suministrada a las bases de datos sea la proporcionada por la persona detenida. En todo caso, la persona detenida será responsable de proporcionar la información de manera correcta y verídica. Las actualizaciones que se realicen al RND deberán ser de manera exacta, completa y correcta, mismas que serán constatadas por la autoridad correspondiente y para las cuales habrá un registro tipo bitácora.

Los sujetos obligados de las instituciones de seguridad pública de los tres órdenes de gobierno tomarán las medidas necesarias para garantizar que las personas adolescentes que sean detenidas reciban un trato conforme a su condición de menor de edad. Esto aplicará tanto para hechos probablemente delictivos, como para faltas administrativas.

SÉPTIMO. FUNCIONES DE LA SECRETARÍA.

Para garantizar el funcionamiento del RND, la Secretaría, a través de la Unidad de Información, Infraestructura Informática y Vinculación Tecnológica, o aquella que defina la persona al frente de dicha Secretaría, tendrá las siguientes funciones:

I. Permitir las condiciones de acceso e interconexión del RND a las instituciones de seguridad pública, específicamente entre las instituciones policiales y aquellas de procuración de justicia;

II. Desarrollar e instrumentar el sistema informático que permita la captura, ingreso, envío, recepción, manejo, actualización, consulta e interconexión del RND;

III. Establecer los criterios para la funcionalidad, operación, respaldo, reconstrucción, seguridad y conservación de la información que integra la base de datos del RND;

IV. Implementar acciones y mecanismos de coordinación para el desarrollo tecnológico y soporte técnico del RND;

V. Recibir las solicitudes de usuario y proporcionar las cuentas conforme a los perfiles y niveles de acceso requeridos por el RND, emitiendo copia de conocimiento al CNI. La solicitud de creación y actualización de cuentas de usuario deberá realizarse de acuerdo a los Lineamientos del SAU y al Catálogo de Perfiles de Usuarios de la SSPC. El tiempo de atención dependerá de la complejidad de la validación de los permisos solicitados con relación al puesto y área de adscripción de la persona servidora pública;

VI. Establecer y mantener actualizadas las medidas de seguridad para el uso del RND, a fin de cuidar el acceso;

VII. Tomar todas las medidas pertinentes para garantizar la disponibilidad, cuidado, conservación y resguardo de la información contenida en la base de dato del RND a partir de que inició dicho registro;

VIII. Operar y mantener actualizados y disponibles el sistema informático y la infraestructura tecnológica para la captura, ingreso, envío, recepción, manejo, actualización, interconexión y consulta del RND. Si el sistema no se encuentra disponible, se informará al SESNSP y a los usuarios sobre las restricciones o suspensiones provisionales del servicio y en su caso, el momento previsto para su restablecimiento;

IX. Adoptar las acciones necesarias para evitar la homonimia en los registros;

X. Permitir que las instituciones de seguridad pública de los tres órdenes de gobierno puedan disponer de la información que hayan proporcionado al RND, para el desarrollo de sus actividades;

XI. Establecer una mesa de servicios que oriente a los usuarios, las 24 horas del día, los 365 días del año, y que pueda dar el seguimiento a los casos a través de un folio;

XII. Ofertar capacitación continua para el uso del RND y su plataforma tecnológica a aquellos elementos de las instituciones de seguridad pública, que por sus funciones, requieran de dichas capacitaciones;

XIII. Guardar constancia de las actualizaciones de la información (bitácora), con la finalidad de identificar al sujeto obligado que la hubiese realizado;

XIV. Emitir certificados digitales sobre los registros de las detenciones y sobre las consultas que realice la autoridad, conforme a sus atribuciones y perfiles de acceso;

XV. Administrar, resguardar e implementar el Sistema de Consulta;

XVI. Emitir certificados digitales sobre los reportes del Sistema de Consulta realizados al RND;

XVII. Colaborar, en la medida de sus posibilidades, con las instituciones de seguridad pública en la implementación de un servicio de interoperabilidad bidireccional, que permita a las entidades y en su caso municipios, interconectar los sistemas de detención propios con los de la Secretaría y viceversa;

XVIII. Llevar a cabo estudios especializados que se desprendan de la información reportada en el RND;

XIX. Comunicar al SESNSP y a las instituciones de seguridad pública encargadas de las tareas de seguridad pública en la federación, las entidades federativas y los municipios, la interrupción del servicio de interoperabilidad bidireccional del RND, ya sea por actualización de la versión o por mantenimiento preventivo en el servicio. En estos casos, la Secretaría tendrá la obligación de que las instituciones de seguridad pública continúen el suministro y la actualización directa de información en el sistema informático del RND; y

XX. Realizar las acciones necesarias para el cumplimiento de los presentes Lineamientos.

OCTAVO. FUNCIONES DEL SESNSP.

Para garantizar el funcionamiento del RND, el SESNSP, a través del CNI, tendrá las siguientes funciones:

I. Elaborar y proponer la actualización o reforma de los presentes Lineamientos, consultando en su caso, a las Conferencias Nacionales, la Comisión Permanente de Información (CPI) del Consejo Nacional de Seguridad Pública (CNSP) y/o a otros actores del Sistema Nacional de Seguridad Pública;

II. Realizar las gestiones necesarias para la publicación de los Lineamientos en el Diario Oficial de la Federación (DOF), así como en otros medios de difusión oficial;

III. Llevar a cabo la interpretación de los Lineamientos, cuando así sea necesario;

IV. Establecer los perfiles y niveles de acceso para la captura, ingreso, envío, recepción, manejo, actualización, y consulta del RND a los que se someterán las instituciones de seguridad pública que realicen detenciones;

V. Emitir recomendaciones a las instituciones de seguridad pública para que implementen procesos ágiles y correctos en la captura y actualización del RND, de conformidad con la Ley y los presentes Lineamientos;

VI. Requerir a las instituciones de seguridad pública que adopten las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en posesión de los sujetos obligados de su adscripción;

VII. Solicitar a las instituciones de seguridad pública la actualización de la información;

VIII. Promover a través de las Conferencias Nacionales, la coordinación y colaboración entre las instituciones de seguridad pública para el cumplimiento de los presentes Lineamientos;

IX. Difundir las buenas prácticas diseñadas e implementadas por las diversas instituciones involucradas en el ámbito del RND, así como colaborar en su promoción de la mano de organizaciones no gubernamentales y de cooperación internacional;

X. Utilizar y, en su caso, compartir la información para realizar estudios especializados y para la integración de la estadística nacional en materia de seguridad pública. El CNI, en acuerdo con las cuatro Conferencias Nacionales del SNSP, podrá también llevar a cabo estudios especializados conjuntos en la materia, previo Acuerdo con sus miembros;

XI. Recibir las copias de conocimiento de las solicitudes de cuentas de usuario que los sujetos obligados requieran a la Secretaría, en cumplimiento con el SAU; y,

XII. Realizar las acciones necesarias para el cumplimiento de los presentes Lineamientos.

NOVENO. OBLIGACIONES DE LAS INSTITUCIONES DE SEGURIDAD PÚBLICA.

Las instituciones policiales, incluyendo a las policías de investigación o cualquier otra que realice o lleve a cabo detenciones, tendrán las siguientes obligaciones:

I. Registrar en el RND todas las detenciones llevadas a cabo en territorio nacional;

II. Asegurar que los sujetos obligados bajo su mando realicen el registro inmediato de la detención (desde el momento en que la persona se encuentra bajo su custodia);

III. Utilizar directamente el sistema informático establecido por la Secretaría para el RND, o, en su caso, interconectar sus sistemas para el intercambio de datos;

IV. Actualizar el servicio de interoperabilidad bidireccional para la integración del RND conforme a las nuevas versiones emitidas por la Secretaría;

V. Continuar el suministro y actualización directa de la información en el supuesto de que el servicio de interoperabilidad bidireccional se vea interrumpido. En este caso, la mesa de servicios deberá apoyar de inmediato a los usuarios y emitir el folio correspondiente a cada incidencia;

VI. Contar con las herramientas electrónicas necesarias para la operación y funcionamiento del RND;

VII. Diseñar e implementar un procedimiento definido para el uso, cuidado y resguardo de las herramientas empleadas para el RND;

VIII. Utilizar únicamente como instrumento de identificación el número de registro de la detención proporcionado por el Sistema;

IX. Capacitar al estado de fuerza para el uso correcto del RND, con los apoyos didácticos proporcionados por la Secretaría;

X. Llenar los campos del RND conforme a los requisitos indicados por el sistema, de acuerdo con la intervención de que se trate (delito o infracción administrativa);

XI. Señalar, según sea el caso, si la persona detenida se identifica como miembro de la delincuencia organizada o si se detuvo por un posible hecho de delincuencia organizada;

XII. Garantizar que la información recabada sea exacta, completa y correcta, de acuerdo con los datos personales proporcionados directamente por la persona detenida;

XIII. Contrastar, en los casos en los que sea posible, la información proporcionada por la persona detenida con otros registros, credenciales de identificación o información oficial;

XIV. Informar inmediatamente a la autoridad que recibe a la persona detenida, sobre aquellos casos en que no le fue posible realizar el registro inmediato, fundando y motivando dicha omisión;

XV. Hacer del conocimiento de la Secretaría, de manera inmediata y a través de la mesa de servicios, cualquier falla en la operación y disponibilidad del sistema. En estos casos, se emitirá un número de folio al que la Secretaría dará puntual seguimiento e informará de su atención a la autoridad interesada;

XVI. Solicitar a la Secretaría la autorización y gestión de las cuentas de usuario, conforme a los perfiles y niveles de acceso que sean requeridos para la adecuada operación del RND, emitiendo copia de conocimiento al CNI;

XVII. Detectar el uso indebido de las cuentas utilizando el perfil de supervisor, y en su caso, solicitar su bloqueo o cancelación;

XVIII. Hacer un uso correcto de las cuentas de usuario proporcionadas por la Secretaría; y,

XIX. Realizar las acciones necesarias para el cumplimiento de los presentes Lineamientos.

La autoridad administrativa, las instituciones de procuración de justicia, y las competentes del sistema penitenciario, tendrán las siguientes obligaciones:

I. Llevar a cabo la actualización de la información en el RND de todas las detenciones que reciban;

II. Utilizar directamente el sistema informático establecido por la Secretaría para el llenado de esta fase del RND, o en su caso, interconectar sus sistemas para el intercambio de datos de dicho registro;

III. Actualizar el servicio de interoperabilidad bidireccional para la integración del RND conforme a las nuevas versiones emitidas por la Secretaría;

IV. Continuar con el suministro y actualización directa de la información en el sistema informático del RND cuando se encuentre interrumpido el servicio de interoperabilidad bidireccional. En estos casos, la mesa de servicios deberá apoyar de inmediato a los usuarios y emitir el folio correspondiente a la incidencia;

V. Asegurar el uso de las herramientas electrónicas necesarias para la operación y funcionamiento del RND;

VI. Garantizar la existencia de un procedimiento definido para el uso, cuidado y resguardo de las herramientas empleadas para el RND;

VII. Utilizar únicamente como instrumento de identificación el número de registro de la detención;

VIII. Capacitar a los sujetos obligados en el uso correcto del RND, con los apoyos didácticos proporcionados por la Secretaría;

IX. Llenar los campos del RND conforme a los requisitos indicados por el sistema, de acuerdo con la etapa del procedimiento penal o administrativo sancionador de que se trate;

X. Procurar que la información de la persona detenida sea exacta, completa y correcta, y contrastar dicha información con otros registros o información oficial;

XI. Iniciar un registro en caso de que no existiese uno previo llevado a cabo por la institución policial;

XII. Informar a las autoridades competentes sobre la falta de registro preexistente;

XIII. Señalar, en su caso, la libertad, el traslado ante otra autoridad, el primer internamiento en una instancia del sistema penitenciario, o el deceso de la persona detenida;

XIV. Hacer del conocimiento de la Secretaría, de manera inmediata, cualquier falla en la operación y disponibilidad del sistema;

XV. Solicitar a la Secretaría la autorización y gestión de las cuentas de usuario, conforme a los perfiles y niveles de acceso que sean requeridos para la adecuada operación del RND, emitiendo copia de conocimiento al CNI;

XVI. Mantener actualizado el padrón de las cuentas de usuarios;

XVII. Proporcionar la información necesaria a la Secretaría para mantener actualizados los catálogos de las agencias del ministerio público del fuero común y federal. Asimismo, mantener actualizada la información de los centros penitenciarios. En el caso de la autoridad administrativa, proporcionar la información de los centros de detención preventiva municipal o similares;

XVIII. Emitir certificados digitales sobre los reportes de los registros de detenciones a través de la herramienta tecnológica que le proporciona la Secretaría;

XIX. Hacer un uso correcto de las cuentas de usuario proporcionadas por la Secretaría; y,

XX. Realizar las acciones necesarias para el cumplimiento de los presentes Lineamientos.

DÉCIMO. NIVELES Y PERFILES DE ACCESO AL RND.

Los niveles y perfiles de acceso al RND serán los siguientes:

I. **Administrador**: Perfil de proceso orientado a los sujetos obligados de la Secretaría y el SESNSP. Su finalidad es realizar funciones adicionales a las operativas y de consulta, como el caso de solicitar altas, bajas y cambios a catálogos, evaluaciones, reportes especiales y configuración de funciones del SNI, conforme a sus atribuciones.

II. **Supervisor**: Perfil orientado a sujetos obligados de las instituciones de seguridad pública que realizan funciones de supervisión sobre la información registrada en el RND, con la finalidad de verificar que sea completa, íntegra y precisa. El supervisor tendrá acceso a los registros capturados por la institución de seguridad pública de adscripción.

III. **Consulta**: Perfil orientado a todos los sujetos obligados que realizan funciones de investigación, inteligencia, análisis de consulta y generación de reportes respecto del RND. Este contará con dos niveles de acceso. El primero se refiere a la consulta estadística, la cual permitirá conocer, de manera agregada, la información que le permita visualizar el estatus nacional de las detenciones. El segundo se refiere a la información desagregada sobre los registros en su entidad federativa como a nivel nacional.

IV. **Capturista**: Perfil orientado a los sujetos obligados de las instituciones de seguridad pública que realizan funciones de captura, ingreso, envío, recepción, manejo y actualización de la información de los datos proporcionados por la persona detenida.

V. **Enlace Estatal o Institucional**: Perfil de proceso orientado a los sujetos obligados que realizan funciones de contacto y tramitan las solicitudes de cuentas de usuario a la Secretaría, conforme a los perfiles y niveles de acceso que se requieran. Este perfil tiene la responsabilidad de mantener actualizado el padrón de las cuentas de usuario.

La Secretaría, el SESNSP, el CNI, las instituciones de seguridad pública de los tres órdenes de gobierno podrán consultar el RND, según su ámbito de competencia, sus perfiles y niveles de acceso.

La Secretaría, a través de la plataforma, emitirá alertas en el sistema y/o por correo electrónico al perfil supervisor, lo que le permitirá dar seguimiento y validar el correcto uso del registro.

DÉCIMO PRIMERO. FUNCIONAMIENTO Y OPERACIÓN DEL RND.

A. EL REGISTRO INMEDIATO.

El registro inmediato constará de la primera información suministrada al RND sobre la detención de una persona. El registro inmediato estará a cargo de las instituciones policiales, incluyendo a las policías de investigación o cualquier otra que realice detenciones. A través de las herramientas electrónicas de las que dispongan para el registro inmediato, los sujetos obligados que tengan el perfil de Capturista del registro inmediato deberán suministrar los siguientes datos en el sistema informático del RND:

I. Nombre(s), apellidos y/o alias;

II. Edad;

III. Nacionalidad;

IV. Fecha y entidad federativa de nacimiento;

V. Sexo;

VI. Descripción de la persona;

VII. Lugar, fecha y hora local en que se haya practicado la detención;

VIII. Los motivos de la detención, señalando si se trata de un presunto hecho delictivo que la ley penal señale o de la presunta infracción administrativa, sin que ello implique una narración de los sucesos. Incluir si la detención obedece al cumplimiento de una orden de aprehensión/mandamiento judicial, detención por flagrancia, reaprehensión, orden de detención con fines de extradición pasiva, reclusión, arraigo, caso urgente o falta administrativa. Si este fuere el caso, se deberá incluir el número de la causa penal o expediente administrativo en el que se emitió la orden de aprehensión, mandamiento judicial u orden de captura;

IX. Nombre de quien o quienes hayan intervenido en la detención, así como la institución, cargo o grado y área de adscripción;

X. La autoridad a la que será puesta a disposición. Ésta deberá precisar el centro penitenciario, la agencia del ministerio público o la autoridad administrativa donde será trasladada la persona detenida;

XI. El nombre y/o teléfono de algún familiar o persona de confianza, en caso de que la persona detenida acceda a proporcionarlo;

XII. El señalamiento de si la persona detenida presenta lesiones apreciables a simple vista;

XIII. La indicación de si se identifica a la persona como miembro de la delincuencia organizada o si se detuvo por un posible hecho de delincuencia organizada; y,

XIV. En caso de que la persona detenida se niegue a proporcionar los datos solicitados, se deberá asentar tal circunstancia en el registro, y capturar la información con la que se cuente.

La información recabada deberá ser exacta, completa y correcta, de acuerdo con los datos personales proporcionados directamente por la persona detenida hasta en tanto se acredite lo contrario.

El registro inmediato se debe realizar previo al traslado de la persona detenida. Este registro no podrá exceder el término máximo de cinco horas contadas a partir de la detención material de la persona, encontrándose bajo la custodia de la institución de seguridad pública que la detuvo. Cuando por algún motivo extraordinario no se pudiera realizar el registro en ese plazo, se hará la justificación relativa en la plataforma y deberá informar de esta situación a la autoridad que realizará la actualización del registro.

En todo momento, los datos personales de las personas físicas identificadas o identificables, estarán sujetos a lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, así como a los supuestos de confidencialidad establecidos en la Ley General de Transparencia y Acceso a la Información Pública, y las demás relativas y aplicables en la materia, con la finalidad de proteger los datos de las personas detenidas.

Una vez realizado el registro inmediato, el sistema generará automáticamente el número de registro de la detención, que servirá para ubicar a través de medios electrónicos a la persona detenida.

Finalizada la captura de la información, el sujeto obligado deberá ingresar la información relacionada con la autoridad a la que será puesta a disposición. Deberá especificar la agencia del ministerio público, el centro penitenciario o la autoridad administrativa donde trasladará a la persona detenida. Si la puesta a disposición no pudo efectuarse por algún motivo, éste deberá expresarse dentro del registro inmediato que realizó el sujeto obligado.

Si después de efectuado el registro inmediato éste no es actualizado por algún sujeto obligado, transcurridos seis días naturales, el registro será cerrado por el sistema y quedará el antecedente correspondiente. En este caso, la Secretaría, a través del sistema informático del RND, emitirá una alerta a la instancia de seguridad pública que realizó el registro inmediato, para que justifique la realización del registro y su falta de actualización, dando aviso al superior jerárquico de los aprehensores, quienes estarán obligados a justificar esta circunstancia y realizar las actuaciones encaminadas a localizar a la persona que estuvo detenida y verificar su integridad física. En tal circunstancia y, de ser procedente, se iniciarán los procedimientos sancionadores que resulten.

En caso de que al momento de la detención, el sujeto obligado no cuente con los medios para capturar la información, éste deberá informar tal situación inmediatamente a la unidad administrativa de su adscripción, por cualquier instrumento del que disponga para que ésta genere el registro.

En caso de que exista demora o resulte imposible generar el registro inmediato, se deberá motivar dicha circunstancia e informarlo inmediatamente a la autoridad que recibe a la persona detenida, para que esta autoridad, de ser necesario, inicie un registro. Este supuesto deberá ser excepcional y la justificación que manifieste el sujeto obligado que no realizó el registro inmediato quedará asentada en el sistema informático.

Los capturistas del registro inmediato tendrán acceso a un tablero, en el cual podrán visualizar los registros generados, organizados por el estado que guarda cada uno de ellos. El supervisor del registro inmediato dará seguimiento a los registros generados por los capturistas en la institución policial de adscripción.

El sistema del RND emitirá alertas, las cuales estarán disponibles para el supervisor a través del mismo sistema y/o mediante correo electrónico. Es responsabilidad del supervisor utilizar esta información para asegurar el uso correcto del registro, dar el seguimiento a dichas alertas e implementar las correcciones necesarias.

B. LA ACTUALIZACIÓN DEL REGISTRO.

La actualización del registro constará de la información complementaria y suministrada al RND sobre la detención o arresto de una persona. La actualización del registro estará a cargo de las autoridades administrativas correspondientes, de las instituciones de procuración de justicia a través del ministerio público y las competentes del sistema penitenciario.

Los sujetos obligados encargados de capturar la información para la actualización podrán visualizar la información capturada, enviada y recibida en el sistema durante la fase previa del registro inmediato. En su caso, podrán ratificar o incorporar información sobre los datos capturados en el registro inmediato, al constatar la veracidad de los datos proporcionados por la persona detenida. Asimismo, el sistema posibilitará la carga de documentos o archivos adjuntos que complementen la actualización del registro.

Cuando el sujeto obligado aprehensor detenga a la persona en ejecución de una orden de aprehensión, reaprehensión, orden de detención con fines de extradición pasiva, o reclusión, y que la persona detenida sea dirigida a la autoridad judicial, la autoridad detenedora será la responsable de realizar la actualización del registro. En el supuesto en el que la persona detenida sea enviada directamente a un centro penitenciario, la autoridad penitenciaria realizará la actualización del registro.

En caso de que se detenga a la persona por la presunta comisión de una falta administrativa, el primer respondiente deberá presentarlo ante la autoridad administrativa, misma que será la responsable de la actualización del registro.

Los sujetos obligados deberán de actualizar el registro dentro del término de dos horas contadas a partir de que la persona detenida es puesta a su disposición material. Para ello, utilizarán las herramientas electrónicas de las que dispongan. De esta forma, los sujetos obligados responsables de la custodia o quienes estén facultados para auxiliarles, capturarán en el sistema informático del RND los siguientes datos:

I. Nombre y cargo del sujeto obligado que actualiza el registro;

II. Autoridad que recibe a la persona detenida, así como el día y hora de la recepción;

III. La indicación de si se identifica a la persona como un presunto miembro de la delincuencia organizada o si se detuvo por un posible hecho de delincuencia organizada; y,

IV. El domicilio de la autoridad que tiene a su disposición a la persona detenida.

Los sujetos obligados deberán de concluir la actualización del registro. Para el caso de probables hechos delictivos, contarán con un plazo máximo de cuarenta y ocho horas a partir de que la persona detenida sea puesta a disposición. En caso de que la detención sea por causa de una presunta falta administrativa, los sujetos obligados contarán con un término máximo de treinta y seis horas contadas a partir de la puesta a disposición. En ambos casos, los sujetos obligados capturarán en el sistema informático del RND los siguientes datos:

I. Los datos de la persona detenida:

- **a.** Lugar y fecha de nacimiento;
- **b.** Sexo;
- **c.** Domicilio;
- **d.** Nacionalidad y lengua nativa;
- **e.** Situación migratoria;
- **f.** Estado civil;
- **g.** Escolaridad;
- **h.** Ocupación o profesión;
- **i.** Clave Única de Registro de Población;
- **j.** Grupo étnico al que pertenezca;
- **k.** Descripción del estado físico de la persona detenida y nombre del médico que certificó o, en su caso, copia del certificado médico;
- **l.** Huellas decadactilares, utilizando como mínimo los estándares internacionales: Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information Part 1; ANSI/NIST-ITL 1-2011, Update 2015, y WSQ Grey-ScalenFingerprint Image Compression Specification, IAFIS-IC-0110, V3;
- **m.** Fotografías de la persona detenida de frente, perfil izquierdo y derecho. Utilizar como mínimo el estándar de captura ISO/IEC 19794-5:2011 Information technology - Biometric data interchange formats - Part 5: Face image data con las últimas actualizaciones, en las especificaciones para fotografías full-frontal. Asimismo, la codificación de la fotografía se debe basar en los siguientes estándares: ISO/IEC 10918-1:1994 Information technology - Digital compression and coding of continuous-tone still images: Requirements and guidelines e ISO/IEC 15444-1:2004 Information technology - JPEG 2000 image coding system: Core coding system. La fotografía se almacenará de acuerdo al tipo lógico 10 (fotografía) al estándar ANSI/NIST-ITL 1-2011 Update 2015; y,
- **n.** En su caso, otros medios que permitan la identificación plena de la persona. Esto incluye los nombres y/o alias que haya proporcionado la persona detenida.

II. Delito o infracción administrativa por el que está detenida la persona;

III. Número de expediente o carpeta de investigación que se integra;

IV. Adicciones, estado general de salud, enfermedades o padecimientos crónicos o degenerativos;

V. Descripción mínima de la ruta de traslado y la autoridad encargada del mismo. Para el caso en el que la persona sea trasladada a otra autoridad, ya sea por motivo de incompetencia o algún otro, se deberá especificar la agencia del ministerio público, autoridad administrativa, centro penitenciario, centro de detención preventiva municipal o similares, unidad especial o la que aplique;

VI. Día y hora de la liberación de la persona detenida; y,

VII. En caso de fallecimiento durante la detención, las circunstancias o causas del deceso y el destino final de la persona fallecida.

Bajo el supuesto de que la detención sea a causa de una presunta falta administrativa, la autoridad administrativa deberá dictar la resolución correspondiente. En caso de ratificar la privación de la libertad, la persona detenida tendrá que ser remitida a un centro de detención municipal, o su equivalente, mismo que deberá realizar la actualización del RND. Si la autoridad administrativa determina dejar en libertad a la persona detenida, esta autoridad será la responsable de actualizar el RND.

En su caso, los sujetos obligados que actualizan el RND podrán cambiar el registro de una falta administrativa, por el registro de un delito, o viceversa, una vez que así lo determine la autoridad obligada a realizar la actualización.

Finalizada la captura de la información no se podrán realizar actualizaciones adicionales.

C. ACTUALIZACIÓN DE INGRESO AL SISTEMA PENITENCIARIO O AL CENTRO DE DETENCIÓN PREVENTIVA MUNICIPAL O SIMILARES.

Los centros penitenciarios y los centros de detención preventiva municipal o lugares de retención de carácter administrativo que reciban a las personas detenidas, deberán solicitar el número de registro de la detención y, con ello, capturar la siguiente información:

I. Nombre y cargo del sujeto obligado que actualiza el registro;

II. Autoridad que recibe a la persona detenida, así como el día y hora de la recepción; y,

III. El domicilio de la autoridad que tiene a su disposición a la persona detenida.

En caso de que sea necesario, los sujetos obligados de los centros penitenciarios y de los centros de detención preventiva municipal o similar, actualizarán la siguiente información de la persona detenida:

I. Nombre(s), apellidos y/o alias;

II. Lugar y fecha de nacimiento;

III. Sexo;

IV. Situación migratoria;

V. Clave Única de Registro de Población (CURP) de la persona detenida;

VI. La indicación de si se identifica a la persona como un presunto miembro de la delincuencia organizada o si se detuvo por un posible hecho de delincuencia organizada; y,

VII. Estado general de salud y condición médica en la que se recibe a la persona.

En el caso de una sanción administrativa, los centros de detención preventiva municipal o similares serán los encargados de recibir al infractor para que cumpla su arresto, mismo que no podrá exceder de 36 horas. Además, estos centros serán los responsables de realizar la actualización del registro una vez que el infractor ingrese al centro de detención preventiva municipal o similares, y al momento en que éste quede en libertad.

En el supuesto de que el ingreso se deba a una orden de aprehensión o de reaprehensión, se deberá suministrar el número de dicha orden. Cuando una persona sea liberada por la autoridad correspondiente, el sujeto obligado deberá actualizar con base en el número de registro de detención, los siguientes datos en el RND:

I. El día de la liberación;

II. La hora de la liberación;

III. El lugar de la liberación;

IV. El responsable de la liberación; y,

V. El motivo de la liberación.

D. ALERTAS DEL SISTEMA.

La Secretaría, a través de la plataforma, emitirá alertas mediante el sistema y/o por correo electrónico al perfil Supervisor, lo que le permitirá dar seguimiento y validar el correcto uso del registro. Dichas alertas permitirán a los Supervisores tomar las medidas necesarias para garantizar el cumplimiento del presente Lineamiento, en el ámbito de la institución de seguridad pública de adscripción. Estas alertas servirán de apoyo al Supervisor para identificar:

I. La manipulación inusual del registro;

II. El incumplimiento de los plazos y tiempos definidos; y,

III. Las situaciones relevantes que ameriten su atención.

E. EXCEPCIÓN DEL REGISTRO.

En caso de que el sujeto obligado aprehensor no haya generado un registro inmediato, el sujeto obligado de la actualización que sea responsable de la persona detenida, deberá iniciar uno propio. Dicho registro se realizará con la información asentada en el IPH, incluyendo los motivos por el cual el sujeto aprehensor omitió el registro inmediato.

Los sujetos obligados de la actualización deberán iniciar el registro dentro del término de dos horas contadas a partir de que la persona detenida es puesta a disposición, y siempre que se encuentre bajo su custodia o de quien está facultado para auxiliarlo. Lo anterior, a fin de cumplir con el objetivo del RND, y con ello, dejar constancia de la autoridad que tiene a su disposición a la persona detenida y el lugar donde será posible localizarla.

En el supuesto de que exista una suspensión temporal del servicio por motivos de fuerza mayor, la Secretaría deberá notificarlo de manera inmediata, mediante un aviso por parte de la mesa de servicios a los enlaces estatales, en la que se establecerá el día y hora exacta de la suspensión del servicio. Esta Constancia será expedida para dar fe del hecho y los efectos legales pertinentes. En este caso, los sujetos obligados ingresarán la información de manera inmediata cuando el sistema reanude su operación. Los sujetos obligados deberán utilizar, en su caso, la información asentada en el IPH incluyendo la certificación de suspensión del servicio que causó la falta de registro inmediato o la actualización del registro.

DÉCIMO SEGUNDO. CONSULTAS DEL RND.

La Secretaría deberá contar con un Sistema de Consulta del RND que permita, por medios tecnológicos, consultar la versión pública de la información de las detenciones practicadas por las instituciones de seguridad pública de los tres niveles de gobierno. Lo anterior, en los términos de la Ley General de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás disposiciones aplicables.

La información de la versión pública que integra el Sistema de Consulta proviene de los datos capturados en el RND por los sujetos obligados. Estos sujetos son los responsables de mantener exactos, completos, correctos y actualizados los datos, de acuerdo con el ámbito de su competencia y de conformidad con los presentes Lineamientos.

El Sistema de Consulta permite ubicar a una persona detenida, a fin de brindar certeza sobre su localización y la institución de seguridad pública que mantiene su custodia. Este sistema emitirá el reporte correspondiente de la persona detenida, el cual deberá contener los siguientes datos, de acuerdo con la información capturada y registrada en el RND:

I. Nombre(s), apellidos y/o alias de la persona detenida;

II. Edad;

III. Media filiación;

IV. La autoridad o institución que efectuó la detención;

V. La autoridad que tiene a su disposición a la persona detenida;

VI. El domicilio del lugar donde se encuentra la persona detenida; y,

VII. Lugar, fecha y hora en que se haya practicado la detención.

Tratándose de presunción de delincuencia organizada únicamente estará disponible la información sobre el nombre de la persona detenida, la fecha de la detención y si la persona aún se encuentra detenida.

En caso de que la plataforma identifique a personas adolescentes, el Sistema de Consulta sólo expondrá las iniciales del nombre de la persona detenida.

La persona interesada que haga uso del Sistema de Consulta deberá ingresar como mínimo, su nombre, primer apellido, una dirección de correo electrónico y teléfono de contacto. Asimismo, para la búsqueda se requerirán el nombre y primer apellido de la persona detenida, fecha y entidad federativa de nacimiento. La plataforma emitirá un certificado digital sobre el reporte que expida el Sistema de Consulta.

Cuando una persona sea liberada por la autoridad correspondiente, la información en el Sistema de Consulta dejará de mostrar de manera pública la información de la detención, transcurridos quince días naturales. En caso de que la persona continúe detenida, transcurridos quince días naturales, la información será cancelada del Sistema Público de Consulta de Detenciones. No obstante, la información quedará en el RND de manera permanente.

El RND podrá ser consultado de acuerdo con lo establecido por la Ley y estos Lineamientos. El objetivo de las consultas será facilitar la información sobre la detención de una persona y su ubicación, así como prevenir la violación de los derechos humanos de la persona detenida y, a su vez, utilizar la base de datos como una herramienta para la seguridad pública.

A. CONSULTA DE LA AUTORIDAD PARA EMITIR CERTIFICADOS DIGITALES.

El perfil de consulta y/o capturista encargado de la actualización de las instituciones de seguridad pública, podrá visualizar y consultar por completo la información del RND capturada, ingresada, enviada, actualizada o consultada por los sujetos obligados, según corresponda.

El sistema informático del RND emitirá certificados digitales sobre los reportes generados de los registros, las detenciones y consultas realizadas, tanto del registro en activo como del histórico. Las instituciones de procuración de justicia encargadas de actualizar el registro, podrán también obtener el certificado digital sobre el reporte generado a fin de cumplir con sus funciones. En ambos casos, dichos certificados servirán para acreditar la existencia o el contenido del registro, así como sus consultas.

La Secretaría determinará la forma y las características del certificado digital, así como los procedimientos para su emisión. Este certificado mostrará el horario del tiempo del centro independientemente del lugar donde sea solicitada la emisión. La información contenida en el reporte certificado será la registrada por los sujetos obligados, y en consecuencia, su contenido será responsabilidad de cada sujeto obligado en cuestión.

B. CONSULTA DE LA PERSONA DETENIDA Y SU REPRESENTANTE LEGAL.

La autoridad competente podrá dar acceso, tanto a la persona detenida como a su representante legal, a la información contenida en el RND.

C. CONSULTA DEL CNI.

Al formar parte del SNI, el RND se integra con la información que las instituciones de seguridad pública de los tres órdenes de gobierno suministran y actualizan mediante los sistemas e instrumentos tecnológicos respectivos.

El CNI podrá utilizar la información del RND para realizar estudios especializados y estadística nacional, en coordinación con otras instancias públicas, así como para generar productos que apoyen la planificación de acciones orientadas a alcanzar los objetivos del SNSP.

D. CONSULTA ESPECIALIZADA.

El perfil de consulta de las instituciones de seguridad pública estatal y federal, o las instituciones de procuración de justicia federal o estatales que designen un enlace con perfil para la consulta especializada, podrán llevar a cabo búsquedas a nivel nacional a fin de realizar inteligencia e investigación. La información que tendrán disponible de la persona detenida será la siguiente:

I. Nombre(s), apellidos y/o alias;

II. Edad;

III. Nacionalidad y lengua nativa;

IV. Fecha y entidad federativa de nacimiento;

V. Sexo;

VI. Clave Única de Registro de Población (CURP);

VII. Situación migratoria;

VIII. Estado civil;

IX. Escolaridad;

X. Ocupación o profesión;

XI. Grupo étnico;

XII. Descripción de la persona; y,

XIII. La indicación de si se identifica a la persona como presunto miembro de la delincuencia organizada o si se detuvo por un posible hecho de delincuencia organizada.

Además, la consulta incluirá información de todas las detenciones que haya tenido la persona en cuestión. En este sentido, la consulta mostrará la siguiente información:

I. Lugar, fecha y hora en la que se haya realizado la detención;

II. Nombre de las instituciones que participaron en la detención;

III. Nombre de las instituciones que tuvieron a disposición a la persona detenida, así como la fecha de ingreso;

IV. Número de carpeta de investigación o expediente administrativo;

V. Número de las órdenes de aprehensión por las que haya sido detenida la persona;

VI. Delito o infracción administrativa por la que fue detenida la persona;

VII. Fotografías;

VIII. Huellas dactilares;

IX. Día y hora de la liberación de la persona detenida; y,

X. En caso de fallecimiento durante la detención o privación de libertad, las circunstancias o causas del deceso y el destino final de la persona fallecida.

La consulta se permitirá a las instituciones de seguridad pública que hayan solicitado debidamente dicho acceso. Asimismo, la Secretaría definirá los requisitos que deberán cumplir los enlaces asignados para obtener dicho perfil.

DÉCIMO TERCERO. CONSERVACIÓN DEL RND.

La conservación del RND se refiere a la ejecución de todas las acciones de mantenimiento necesarias para el óptimo estado, funcionamiento y operación, para el cuidado y resguardo de la información almacenada en su base de datos.

La Secretaría será la responsable de conservar la infraestructura tecnológica, el sistema informático y la base de datos del RND. Ésta tendrá la obligación de contar con un protocolo específico para establecer y mantener actualizadas las medidas de seguridad necesarias para la conservación del RND, la protección de los datos personales, así como el acceso y ejercicio de los Derechos de Acceso, Rectificación, Cancelación y

Oposición (Derechos ARCO), que señalan la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Tanto la Secretaría, como los demás sujetos obligados en los presentes Lineamientos, deberán cumplir con el marco normativo de protección a datos personales, y en su caso, a cualquier dato biométrico vinculado al RND.

La Secretaría y el SESNSP de manera conjunta, o por separado, y con base en sus facultades, establecerán las políticas de acceso y uso de la información del RND, previa consulta con la Conferencia Nacional de Procuración de Justicia sobre los casos en los que compartir información ponga en riesgo el curso de alguna investigación. Lo anterior, a fin de proteger la integridad de los datos registrados y evitar su mal uso.

La Secretaría guardará una bitácora de los accesos a la base de datos, con la finalidad de identificar al servidor público que acceda y el tipo de actividad que realiza.

DÉCIMO CUARTO. VINCULACIÓN CON OTRAS BASES DE DATOS.

El RND podrá estar enlazado con otras bases de datos del SNI a través del número de registro de la detención o mediante aquellos datos que sean compatibles entre sí. Lo anterior, permite que la información contenida en el RND pueda ser utilizada para el fortalecimiento de la estrategia de seguridad pública, de conformidad con la normatividad aplicable.

Los usuarios del sistema informático del RND que pertenezcan a las instituciones de seguridad pública, deberán estar vinculados con el RNPSP. El RND podrá vincularse con otras bases de personal para el caso de actores que no estén incluidos en este registro.

DÉCIMO QUINTO. INCUMPLIMIENTO DE LOS LINEAMIENTOS.

El incumplimiento de estos Lineamientos podrá traer consigo las responsabilidades penales, administrativas y de cualquier otra índole a que haya lugar de conformidad con las leyes aplicables. Lo anterior, de acuerdo con las facultades y obligaciones de los servidores públicos señalados como responsables de su aplicación.

En caso de que un servidor público tenga conocimiento de algún incumplimiento, deberá hacerlo del conocimiento de su superior jerárquico inmediato, dejando constancia para que, en su caso, se tomen las acciones procedentes. La institución a la que pertenezca el servidor público denunciante deberá tomar las medidas necesarias para su protección.

TRANSITORIOS

PRIMERO. Los presentes Lineamientos entrarán en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

SEGUNDO. Las autoridades municipales que realizan detenciones, tendrán un plazo máximo de 18 meses a partir de la publicación de estos Lineamientos para la implementación completa del registro, en su modalidad de justicia cívica.

TERCERO. Los sujetos obligados responsables de los centros penitenciarios, así como de los centros de detención preventiva municipales o similares que reciben detenciones, tendrán un plazo máximo de 18 meses a partir de la publicación de estos Lineamientos para llevar a cabo la actualización de la información de todas las detenciones en el RND.

CUARTO. Los sujetos obligados que conforman el registro, según lo establecido en los numerales B y C del Lineamiento Décimo Primero, tendrán un plazo máximo de 36 meses a partir de la publicación de estos Lineamientos para la implementación de los biométricos.

QUINTO. La Secretaría tendrá un plazo máximo de 18 meses a partir de la publicación de estos Lineamientos para implementar la consulta especializada.

SEXTO. Se abrogan los Lineamientos para el funcionamiento, operación y conservación del Registro Nacional de Detenciones, publicados el 22 de noviembre de 2019 en el DOF, así como todas las disposiciones que se opongan a los presentes Lineamientos.

Dado en la Ciudad de Villahermosa, Tabasco, a los 16 días del mes de diciembre de dos mil veintiuno.- El Titular del Centro Nacional de Información, **Jesús David Pérez Esparza**.- Rúbrica.

ANEXO 2 del Acuerdo 09/XLVII/21 del Consejo Nacional de Seguridad Pública, aprobado en su Cuadragésima Séptima Sesión Ordinaria, celebrada el 16 de diciembre de 2021, publicado el 29 de diciembre de 2021.

Al margen un logotipo, que dice: Secretaría de Seguridad y Protección Ciudadana (SSPC).- Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP).- Centro Nacional de Información (CNI).

Nuevos Lineamientos del Sistema de Administración de Usuarios (SAU)

JESÚS DAVID PÉREZ ESPARZA, Titular del Centro Nacional de Información (CNI) del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), atendiendo a lo establecido por los artículos 21, párrafos noveno y décimo de la Constitución Política de los Estados Unidos Mexicanos; 1, 5, fracción II, 7 fracción IX, 17, 19, 39 Apartado B, fracciones V y VI, 109 y 110 de la Ley General del Sistema Nacional de Seguridad Pública; 1, 4, 6, fracción III, 8, fracción IV, 10, 11, fracciones I, XV, XVII y 12 fracciones III, XX, XXII y XXIV del Reglamento del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, y

CONSIDERANDO

Que el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos dispone que la seguridad pública es una función del Estado a cargo de la federación, las entidades federativas y los municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia. La seguridad pública comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución;

Que el párrafo noveno y décimo, inciso b), del artículo constitucional antes señalado, dispone que la federación, las entidades federativas y los municipios, se coordinarán en los términos que la ley señale, para establecer un Sistema Nacional de Seguridad Pública (SNSP);

Que el artículo 5, fracción II de la Ley General del Sistema Nacional de Seguridad Pública (LGSNSP), dispone que las bases de datos del Sistema Nacional de Información en Seguridad Pública (SNI), constituyen subconjuntos sistematizados de la información contenida en Registros Nacionales en materias relativas a detenciones, armamento, equipo y personal de seguridad pública, medidas cautelares, soluciones alternas y formas de terminación anticipada, así como las bases de datos del Ministerio Público y las instituciones policiales de los tres órdenes de gobierno relativas a la información criminalística, huellas dactilares de personas sujetas a un proceso o investigación penal, teléfonos celulares, personas sentenciadas y servicios de seguridad privada, así como las demás necesarias para la prevención, investigación y persecución de los delitos.

Que de conformidad con el artículo 7, fracción IX, 39, Apartado B, fracciones V y VI, de la Ley antes señalada, la federación, las entidades federativas, y los municipios deben compartir, intercambiar, ingresar, almacenar y proveer información, archivos y contenidos a las bases de datos que integran el SNI, así como garantizar la interconexión y consulta, y designar un responsable del control, suministro y adecuado manejo de la información a que se refiere esta Ley;

Que de acuerdo con los artículos 19 de la LGSNSP y 12 fracción III del Reglamento del SESNSP, el CNI es el responsable de regular el SNI y le compete entre otras atribuciones, vigilar el cumplimiento de los criterios de acceso a la información, y hacer del conocimiento de las instancias competentes cualquier irregularidad detectada, actualizar las bases de datos del SNI, así como crear, operar y actualizar de forma permanente un padrón de servidores públicos de los tres órdenes de gobierno que suministren, actualicen o consulten las bases de datos del SNI, y llevar bitácoras de su acceso;

Que según lo dispuesto por el artículo 109 de esta misma Ley, el CNI podrá utilizar las bases de datos del SNI para generar productos que apoyen la planificación de acciones orientadas a alcanzar los objetivos del SNSP. El acceso al SNI estará condicionado al cumplimiento de esta Ley, los acuerdos generales, los convenios y demás disposiciones que de la propia Ley emanen;

Que de conformidad con el artículo 110 de esta misma Ley, la información contenida en las bases de datos del SNI, podrá ser certificada por la autoridad respectiva y tendrá el valor probatorio que las disposiciones legales determinen. Se clasifica como reservada la información contenida en todas y cada una de las bases de datos del SNI, así como los registros nacionales y la información contenida en ellos.

Que según lo dispuesto en el artículo 117 de la LGSNSP, la federación, las entidades federativas y los municipios serán responsables de integrar y actualizar el SNI, con la información que generen las Instituciones de Procuración de Justicia e Instituciones Policiales, que coadyuve a salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos, mediante la prevención, persecución y sanción de las infracciones y delitos, así como la reinserción social;

Que conforme a lo dispuesto en los artículos 1, 6 y 7 de la Ley del Registro Público Vehicular (REPUVE), este Registro es un instrumento de información del SNSP que tiene como propósito otorgar seguridad pública y jurídica a los actos que se realicen con los vehículos en el territorio nacional, integrando y compartiendo la información que proporcionan las autoridades federales, las entidades federativas y los Sujetos Obligados por dicha Ley;

Que los artículos 4 y 5 del Reglamento de la Ley del REPUVE, disponen que el SESNSP establecerá un padrón de Sujetos Obligados, en el que dará de alta o baja los datos de identificación de quienes inscriban vehículos o den avisos al Registro, así como la definición de los procedimientos de operación que deberán cumplir los Sujetos Obligados para el acceso, suministro, intercambio y sistematización de la información que entregarán al REPUVE;

Que de acuerdo con el artículo 12 del Reglamento Interior de la SSPC, corresponde a la Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico (DGGSCDT), administrar a los usuarios que operan las bases de datos criminalísticas y de personal contenidos en la Plataforma México;

Que el octavo objetivo de la Estrategia Nacional de Seguridad Pública plantea utilizar mecanismos de inteligencia en busca de construir una paz duradera y fructífera, para lo cual una regulación apropiada del acceso a las distintas bases de datos que conforman el SNI se vuelve vital;

Que la administración 2018-2024 tiene entre sus prioridades la implementación del Modelo Nacional de Policía y Justicia Cívica, con el que se busca la consolidación de áreas dedicadas a la investigación del delito, haciendo uso de datos veraces, completos y oportunos;

Que el 8 de julio de 2010, el CNI publicó en el Diario Oficial de la Federación (DOF) los primeros Lineamientos para la inscripción y baja en el SAU;

Que los Lineamientos del SAU tienen la finalidad de regular el acceso de las instituciones de seguridad pública a las bases de datos que integran el Sistema Nacional de Información;

Que con fecha de 16 de diciembre de 2021, el Consejo Nacional de Seguridad Pública (CNSP), a través del Acuerdo 09/XLVII/21, aprobó e instruyó la publicación de los presentes Lineamientos; y,

Que en función de lo anterior, he tenido a bien emitir el siguiente:

ACUERDO POR EL QUE SE ACTUALIZAN LOS LINEAMIENTOS PARA LA INSCRIPCIÓN Y BAJA EN EL SISTEMA DE ADMINISTRACIÓN DE USUARIOS (SAU) DEL PERSONAL DESIGNADO COMO RESPONSABLE DEL CONTROL, SUMINISTRO, INTERCAMBIO, ACTUALIZACIÓN Y ADECUADO MANEJO DE LA INFORMACIÓN DE LAS BASES DE DATOS DEL SISTEMA NACIONAL DE INFORMACIÓN (SNI) EN SEGURIDAD PÚBLICA

1. OBJETIVO

Garantizar una administración centralizada y segura de los usuarios de los sistemas informáticos que utiliza el SNI, gestionando los diferentes perfiles que facultan a los usuarios para integrar, consultar y actualizar la información en el ámbito de su competencia, además de conformar bitácoras de sus actividades.

2. ÁMBITO DE APLICACIÓN

Los lineamientos descritos en este documento deberán observarse por las dependencias, instituciones, personas físicas y morales que se listan a continuación:

a) Instituciones de Seguridad Pública en los tres ámbitos de gobierno;

b) Fiscalía General de la República; Fiscalía General de Justicia de la Ciudad de México, así como a las Fiscalías Generales de Justicia Estatales o sus equivalentes;

c) Secretaría de la Defensa Nacional;

d) Secretaría de Marina Armada de México;

e) Centros de Reclusión Federal o de las entidades federativas, así como los centros de detención municipal o similares;

f) Centros de Certificación, de Acreditación y Control de Confianza u homólogos;

g) Academias de Seguridad Pública y Procuración de Justicia o similares;

h) Todas aquellas dependencias del Gobierno Federal, de las entidades federativas y municipios que, a partir de sus atribuciones y obligaciones legales, y que, por sus actividades vinculadas a la seguridad pública, requieran acceso a los Sistemas de Información del SNI y a la base de datos del Registro Público Vehicular (REPUVE); y,

i) Sujetos Obligados del REPUVE.

3. DEFINICIONES

Anexo Formato Único: Formato adicional a la cédula única del registro de usuarios. En éste se indican los datos personales, adscripción, fotografías y huellas dactilares de la persona funcionaria pública que solicita el alta de una cuenta de usuario. Este anexo será requerido para el personal que no está inscrito en el Registro Nacional de Personal de Seguridad Pública (RNPSP).

Área de Administración de Usuarios (AAU): La DGGSCDT de la SSPC es el área responsable de los procedimientos informáticos para dar de alta, baja o modificar las cuentas de usuarios.

Catálogo de Firmas: Formato en el que se indican los datos de la(s) persona(s) responsable(s) de la entidad federativa o institución para solicitar el alta, modificación, ampliación o reactivación de una cuenta de usuario.

Catálogo de Perfiles: Listado y descripción de los Perfiles de Usuario existentes para el acceso al SNI.

Cédula de Inscripción de Usuarios (CIU) del REPUVE: Formato en el que se indican los datos personales, laborales y fotografía de una persona empleada por parte de un sujeto obligado para solicitar una cuenta de usuario que le permita suministrar, actualizar o consultar datos específicos en los Sistemas de Información del REPUVE.

Cédula Única de Registro de Usuarios: Formato en el que se indican los datos personales, adscripción y perfiles de usuario para solicitar el alta, modificación, ampliación o reactivación de una cuenta de usuario.

Clave Única de Identificación Permanente (CUIP): Clave generada por el RNPSP para todas las personas que pertenezcan a alguna institución o corporación relacionada con la seguridad pública.

CNI: Centro Nacional de Información.

Contraseña: Palabra secreta, conformada por letras y números, que permite a un usuario ingresar al SNI.

Control de Confianza: Las evaluaciones de control de confianza son las que se aplican con fines de nuevo ingreso, permanencia o periódicas u orientadas a casos particulares para la toma de decisiones con efectos de ascenso, asignación de nuevas responsabilidades, funciones especializadas y/o accesos de información confidencial, así como acciones de capacitación. Los criterios para su realización están dados a conocer a través de la página del SESNSP.

Cuenta de usuario: Identificación personal e intransferible que utiliza un Usuario en combinación con su contraseña para ingresar a los Sistemas de Información del SNI o a los Sistemas de Información del REPUVE.

DGGSCDT: Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico de la SSPC.

Digitalización: Proceso mediante el cual las instituciones, a través de los Enlaces, ingresan la información y documentación (física o medio digital) requisitada para el trámite sistematizado de las cuentas de usuarios.

Enlace Estatal o Institucional: Persona autorizada para tramitar las solicitudes de cuentas de usuarios de una entidad federativa o institución.

Instituciones: Las instituciones de seguridad pública y procuración de justicia.

LGSNSP: Ley General del Sistema Nacional de Seguridad Pública.

Perfil de Usuario: Personalidad que engloba el conjunto de opciones que puede realizar un usuario en los Sistemas de Información del SNI o del REPUVE, según sus atribuciones y obligaciones legales.

REPUVE: El Registro Público Vehicular tiene por objeto la identificación y control vehicular; en la que consten las inscripciones o altas, bajas, emplacamientos, infracciones, pérdidas, robos, recuperaciones y destrucción de los vehículos que se fabrican, ensamblan, importan o circulan en el territorio nacional, así como brindar servicios de información al público.

RNPSP: Registro Nacional de Personal de Seguridad Pública.

SESNSP: Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.

Sistema de Administración de Usuarios (SAU): Mecanismo que, al conjuntar elementos tecnológicos y administrativos, garantiza que la información y las aplicaciones informáticas del Sistema Nacional de Información sólo sean utilizadas por personas autorizadas y siempre de acuerdo con sus atribuciones y obligaciones legales. El SAU es el único mecanismo para realizar altas, modificaciones o bajas (vencimiento, suspensión y cancelación) de usuarios.

Sistemas de Información del Registro Público Vehicular: Herramientas informáticas con las que se realiza el suministro, la actualización o las consultas de la información contenida en las bases de datos del REPUVE.

Sistemas de Información del Sistema Nacional de Información: Herramientas informáticas con las que se realiza el suministro, la actualización o las consultas de la información contenida en las bases de datos del SNI.

SNI: Sistema Nacional de Información en Seguridad Pública.

SNSP: Sistema Nacional de Seguridad Pública.

SSPC: Secretaría de Seguridad y Protección Ciudadana.

Sujetos Obligados: Aquellos enumerados en la Ley del REPUVE y que tienen la obligación de suministrar, actualizar o consultar información en los Sistemas de Información del REPUVE.

Usuario: Persona autorizada que, de acuerdo con sus funciones, puede acceder, suministrar, actualizar o consultar los datos que proporcionan los Sistemas de Información del SNI.

4. DISPOSICIONES GENERALES

El Centro Nacional de Información (CNI) deberá:

a) Generar y difundir el catálogo de perfiles.

b) Vigilar el estatus de las solicitudes de alta, baja o modificación de usuarios en las bases de datos del SAU realizadas a través del enlace estatal o institucional. Para dicho efecto, estas solicitudes se digitalizarán y atenderán por el AAU, según el ámbito de aplicación de los presentes Lineamientos.

c) Contar con el padrón de usuarios actualizado.

Las instituciones deberán:

a) Realizar las solicitudes, tramitar y administrar el seguimiento ante el AAU, remitiendo copia de conocimiento al CNI o al REPUVE, según sea el caso.

b) Solicitar mediante oficio (físico o medio digital), el alta, baja o modificación de usuarios, anexando la documentación requerida. Ésta deberá evitar enmendaduras, tachaduras y deberá estar debidamente requisitada conforme a los presentes lineamientos.

c) Garantizar el uso correcto y apegado a derecho del SNI.

El Registro Público Vehicular deberá:

a) Difundir un catálogo de perfiles específico para los sujetos obligados.

b) Analizar y validar las peticiones realizadas por los sujetos obligados, en un plazo no mayor a 15 días naturales. En caso de que el sujeto obligado no cumpla con algún detalle en la documentación o expediente, el REPUVE deberá notificar al sujeto obligado el faltante a su expediente.

c) Gestionar directamente la petición ante el AAU a través de control de gestión de la Unidad.

d) Enviar al AAU, el oficio de solicitud emitido por el REPUVE, la CIU y el formato de alta, baja o actualización al Padrón.

Los Sujetos Obligados del REPUVE deberán:

a) Solicitar mediante oficio dirigido al REPUVE, el alta, baja o modificación de usuarios para cumplir sus obligaciones, anexando la documentación requerida (física o medio digital). Ésta deberá ser clara, legible, sin enmendaduras o tachaduras, debidamente requisitada conforme a los presentes Lineamientos. Con ello, el REPUVE enviará la solicitud correspondiente al AAU mediante oficio.

b) Conocer las aplicaciones informáticas a las que tendrán acceso.

c) Conocer los alcances legales y sus efectos en caso de hacer uso indebido de la información.

El Área de Administración de Usuarios (AAU) deberá:

a) Recibir de los Enlaces o del REPUVE las solicitudes con la documentación soporte (física o medio digital) que acredite la aprobación de alta o modificaciones de cuentas de usuarios, de acuerdo con su ámbito de aplicación.

b) Asegurar que las entidades federativas, instituciones y, en su caso, sujetos obligados, cubran los requisitos documentales y vigilar la veracidad de dicha documentación.

c) Realizar los procedimientos técnicos necesarios para dar de alta, baja o modificar las cuentas de usuario con los perfiles solicitados.

d) Asignar a cada cuenta de usuario su correspondiente contraseña para el acceso al Sistema de Información del SNI o al del REPUVE, según corresponda.

e) Enviar al personal designado oficialmente como Enlace Institucional, vía correo electrónico institucional, un archivo cifrado con la cuenta del usuario y la contraseña.

f) Notificar vía correo electrónico al sujeto obligado, marcando copia de conocimiento al REPUVE, una vez que sea atendida la solicitud. Se hará lo propio con el CNI al respecto de las instituciones en el ámbito de aplicación de los presentes Lineamientos.

g) Rechazar el trámite en caso de detectar el incumplimiento en una o más de las especificaciones establecidas en los presentes lineamientos.

h) Atender las solicitudes enviadas por el REPUVE, en un plazo no mayor a 15 días naturales a partir de haber recibido la solicitud.

i) Conformar un padrón de usuarios de los sistemas de información del SNI y del REPUVE.

j) Conformar un padrón de funcionarios facultados para solicitar el alta de nuevos usuarios.

k) Administrar la información de las bitácoras de actividades de los usuarios en el Sistema de Información del SNI y del REPUVE.

l) Bloquear las cuentas de usuario con actividad sospechosa (virus, conexión en sitios diferentes, duplicidad en la conexión, entre otras irregularidades similares), que pudieran significar una amenaza que comprometa la seguridad de la información e infraestructura del SNI, así como las cuentas de usuarios que no tengan actividad por un periodo mayor a 6 meses. De reiterarse una actividad sospechosa de alguna cuenta de usuario, ésta se dará de baja y se notificará por correo electrónico al enlace estatal o institucional y al CNI.

m) Habilitar el acceso del CNI a la base de datos del SAU, en modo consulta por medio de su aplicativo, con el propósito de vigilar el cumplimiento de los criterios de acceso a la información y hacer del conocimiento a las instancias competentes cualquier irregularidad detectada.

Los Enlaces Institucionales deberán:

a) Mantener vigentes y aprobados los exámenes de control de confianza.

b) Validar la cédula única o anexo único, mismos que deberán estar debidamente requisitados. Las personas autorizadas para firmar la cédula única o formato único deberán incluir su firma autógrafa tal y como la enviaron en el formato del catálogo de firmas, además de la rúbrica.

c) Enviar digitalmente el documento que acredite los exámenes de control y confianza vigentes y aprobados de la persona servidora pública que solicita la cuenta de usuario.

d) Recabar las firmas de los servidores públicos responsables de autorizar las solicitudes de las cuentas de usuario, mediante el formato del catálogo de firmas, e informar al AAU.

e) Validar que los perfiles indicados en la cédula única sean de la competencia de la institución a la que está adscrito el usuario, según el catálogo de perfiles publicado por el CNI.

f) Notificar la baja de un usuario. Para dicho fin, el Enlace Institucional deberá enviar el documento correspondiente al AAU, en un periodo no mayor a 24 horas después de la baja del usuario en cuestión.

El Enlace Institucional deberá considerar lo siguiente:

a) Adecuar los privilegios conforme a la petición de modificación de perfiles.

b) Especificar en la cédula única los casos en los que una persona está adscrita a la Unidad de Análisis de Información (UDAI).

c) Indicar en la cédula única, los casos en los que el usuario se encuentra Comisionado, es decir, que ha sido asignado temporalmente a otra tarea, área o institución.

d) Indicar en el oficio de petición, para el caso de perfiles biométricos, las direcciones IP de los equipos, la entidad y las adscripciones.

Requisitos para la asignación de Enlaces Institucionales:

a) Solicitar mediante oficio (físico o medio digital), la designación de la persona que fungirá como Enlace Institucional. Éste será el que realice todas las solicitudes de cuentas de usuario de su institución.

b) Anexar el formato de catálogo de firmas en el oficio de solicitud. Éste llevará la firma del responsable que autoriza las cuentas de usuario.

c) Anexar en el oficio solicitud el formato de cédula única. Éste deberá estar debidamente requisitado, firmado y sellado conforme a los presentes Lineamientos.

Los usuarios deberán:

a) Hacer uso correcto de su cuenta y contraseña conociendo que éstas son personales e intransferibles.

b) Hacer uso correcto de los Sistemas de Información del SNI o del REPUVE, ya que de no hacerlo se harán acreedores a las sanciones indicadas en el artículo 139 de la LGSNSP.

5. DEL ALTA DE USUARIOS

Las instituciones y los sujetos obligados del REPUVE realizarán el trámite de alta, modificación, reactivación y baja de usuarios mediante oficio (físico o medio digital). Éste deberá ser dirigido al AAU.

Para convertirse en usuario, toda persona que pertenezca a una Institución de Seguridad Pública deberá estar inscrita y con estatus de activo en el RNPSP conforme al artículo 122 de la LGSNSP. Para dicho trámite, la documentación obligatoria para el alta de cuentas de usuario de estos servidores públicos será:

a) El oficio (físico o medio digital) de solicitud dirigido al AAU.

b) La cédula única de registro de usuarios con las siguientes características:

- Tipos de perfiles de usuarios.
- Oficio de solicitud firmado por el servidor público solicitante, el responsable de la institución y el Enlace Institucional. Este oficio deberá llevar el sello institucional de la dependencia. En caso de no contar con sello, esto deberá ser mencionado en el oficio de la solicitud.
- Contar con la CUIP del usuario, misma que deberá especificarse en la cédula única de registro de usuarios. La CUIP deberá coincidir con la registrada en el RNPSP.

c) El Catálogo de Firmas de la o las personas servidoras públicas que autorizan el trámite. Es decir, la persona responsable de la institución y Enlace Institucional.

d) Para el caso del personal que solicita usuario, el Enlace Institucional deberá anexar el documento emitido por el Centro de Control de Confianza correspondiente. En éste se deberá indicar que el personal mantiene las evaluaciones de control de confianza aprobada y vigente, y que cumple con los requisitos establecidos por la norma aplicable. El documento se validará por el AAU y lo hará de conocimiento al CNI.

La documentación obligatoria para el alta de cuentas de usuario para funcionarios públicos no inscritos en el RNPSP será:

a) Oficio (físico o medio digital) de solicitud dirigido al AAU.

b) Cédula Única de Registro de Usuarios, indicando el perfil que solicita. Ésta deberá estar firmada por el funcionario público solicitante, el responsable de la institución y el Enlace Institucional. Además, deberá presentar el sello de la dependencia. En caso de no contar con éste, deberá mencionarlo en el documento.

c) Anexo del formato único debidamente requisitado.

d) Copia simple de identificación oficial vigente del usuario (Credencial INE, Pasaporte, Cédula Profesional).

e) Catálogo de firmas de la persona funcionaria pública que autoriza el trámite.

Referente a las cuentas de usuario del personal de un Sujeto Obligado, se deberá cumplir con los requisitos establecidos por el REPUVE, siendo éstos:

a) Carta de petición de trámite de alta de usuario dirigida al REPUVE.

b) Cédula de Inscripción de Usuarios al REPUVE.

c) Formato de Alta al Padrón de Sujetos Obligados.

d) Copia simple de Identificación oficial vigente del usuario (Credencial INE, Pasaporte, Cédula Profesional).

e) Copia simple del comprobante de domicilio con fecha de expedición. Éste no podrá ser mayor a tres meses anteriores al día de su presentación.

f) Constancia laboral en original, indicando la fecha de ingreso al trabajo. En caso de ser subcontratado, deberá indicarse que está asignado al Sujeto Obligado que solicita su alta.

La información será validada por el REPUVE y éste solicitará al AAU cualquier corrección necesaria.

La documentación no deberá presentar tachaduras o enmendaduras. Ésta deberá llenarse de forma completa, apegándose a las instrucciones establecidas en el propio formato.

El AAU emitirá una comunicación electrónica al Enlace Institucional, sobre la aceptación o rechazo de las solicitudes. El AAU será responsable de hacer llegar la cuenta de usuario al servidor público solicitante.

Una vez emitida la comunicación de la aceptación de alta de una cuenta de usuario, éste tendrá un plazo de cuatro meses para hacer uso de ésta. De no ser así, dicha cuenta será dada de baja.

En todos los casos, las instituciones involucradas y los sujetos obligados deberán realizar el proceso de validación y/o verificación física de la documentación que les sea solicitada.

6. MOTIVOS DE RECHAZO

a) Cuando la CUIP registrada en la cédula única no corresponda con la registrada en el RNPSP.

b) Cuando la cédula única no contenga la CUIP. Este escenario aplica para las instituciones definidas en el glosario de estos Lineamientos.

c) Cuando los perfiles registrados en la cédula única o el formato único sean diferentes al oficio solicitud.

d) Cuando el nombre de la persona registrada en la cédula única o el formato único no coincida con el del RNPSP. La excepción aplicaría cuando el CUIP registrado en su formato único sí coincida con el del RNPSP. En este caso, se debe corregir el nombre y garantizar que el usuario firme su formato con el nombre correcto.

e) Cuando la cédula única no tenga registrado perfil alguno. La excepción aplicaría cuando se esté solicitando el alta de un Enlace Institucional.

f) Cuando la cédula única o el formato único sean llenados de forma combinada. Es decir, a máquina y a mano, o utilizando diferentes colores.

g) Cuando la cédula única no esté firmada por el Enlace Institucional.

h) Cuando la cédula única no esté firmada por el responsable de la institución.

i) Cuando la cédula única o el formato único no estén firmados por los usuarios solicitantes.

j) Cuando la cédula única o el formato único, en los apartados de las firmas, les falte algún dato de los que se especifican. Por ejemplo: nombre completo, cargo y firma.

k) Cuando la cédula única o el formato único original sea ilegible o se confundan letras o números.

l) Cuando el responsable que firma la cédula única o el formato único no esté registrado en el catálogo de firmas y éste no sea anexado en la documentación.

m) Cuando no se cuente con el oficio solicitud correspondiente de la institución.

n) Cuando los perfiles indicados en la cédula única o el formato único no le correspondan al usuario.

o) Cuando no se indique en la cédula única el tipo de movimiento que solicitan. Por ejemplo: nueva cuenta, modificación de perfil, ampliación de perfil, reactivación de cuenta o cambio de adscripción.

p) Cuando la AAU solicite la validación al Enlace Institucional de alguna de las áreas de adscripción y no exista una respuesta en un lapso mayor a 72 horas.

q) Cuando la cédula única o el formato único presenten tachaduras o enmendaduras.

r) Cuando la cédula única o el formato único sean alterados en su formato, o bien, sean formatos caducos.

s) Cuando el usuario se encuentre con estatus diferente a Activo en el RNPSP.

Las solicitudes que incumplan algún requisito de los mencionados en los presentes Lineamientos, no serán procesadas.

7. DEL PERFIL Y CONTRASEÑA

a) La asignación de cuentas de usuario y contraseña se controlará mediante el SAU.

b) La cuenta de usuario y contraseña tendrá carácter personal, único e intransferible. El mal uso de éstas, podría ocasionar que el solicitante se haga acreedor a las sanciones indicadas en el artículo 139 de la LGSNSP.

c) La contraseña deberá estar conformada por ocho caracteres, además de contener al menos una letra mayúscula exceptuando la O, L, I, J, Ñ, y los números 0 (cero) y 1 (uno).

d) El tiempo para la generación de cuentas de usuario y contraseña será el que determine el AAU. Esto dependerá de la complejidad del trámite.

e) Es responsabilidad del usuario cambiar su contraseña directamente en la herramienta tecnológica cuando la reciba por primera vez, cuando lo considere necesario o antes del término de la vigencia.

f) Las contraseñas tendrán una vigencia de 90 días. Antes de cumplirse este plazo, será responsabilidad del usuario cambiar la contraseña. De no hacerlo, la cuenta quedará bloqueada. Para lograr el cambio de contraseña, el AAU deberá proporcionar la herramienta tecnológica correspondiente.

g) El usuario podrá solicitar, máximo tres veces al mes, el cambio de contraseña a través del AAU. Ésta deberá verificar fehacientemente que el solicitante es quien fue registrado como usuario. En caso de detectarse usurpación de persona, la cuenta de usuario en cuestión será bloqueada y en caso de reincidencia, será dada de baja de manera definitiva.

h) El usuario no deberá iniciar o mantener abierta más de una sesión, en más de un equipo, en forma simultánea.

i) El usuario tendrá hasta 3 intentos para colocar su contraseña. Si los excede, la cuenta quedará bloqueada.

j) La asignación de perfiles se otorgará con base en el catálogo de perfiles vigentes.

8. DE LA BAJA DE USUARIOS

Los titulares de las instituciones y los sujetos obligados serán responsables de las bajas y cambios de adscripción de los usuarios. Para ello, deberán notificar por oficio, en un plazo no mayor a 24 horas, la causa o motivo de dicha baja, el cambio de adscripción y la fecha.

En caso de incumplimiento a lo indicado en el párrafo anterior y, que como resultado de ello se haya provocado el mal uso de una cuenta de usuario, los funcionarios públicos señalados se harán acreedores a las sanciones indicadas en el artículo 139 de la LGSNSP.

El AAU realizará la baja definitiva de una cuenta de usuario cuando reciba la solicitud de baja enviada por el Enlace Institucional. Una vez realizada la baja, se notificará por correo electrónico al Enlace Institucional y al CNI.

El AAU realizará la baja definitiva de una cuenta de usuario al detectar que el titular de dicha cuenta tiene estatus de inactivo en el RNPSP. En este caso, el AAU notificará por correo electrónico al Enlace Institucional y al CNI.

El AAU realizará la baja definitiva de una cuenta de usuario al detectar, por medio de las bitácoras de actividad de los Sistemas de Información del SNI y del REPUVE, el uso inadecuado de la misma o la falta de actividad por un periodo mayor a 12 meses. Una vez realizada la baja, el AAU notificará por correo electrónico al Enlace Institucional y al CNI.

9. DE LA BITÁCORA DE ACTIVIDADES DE LOS USUARIOS

Toda consulta, actualización y/o modificación a la información de las bases de datos del SNI y del REPUVE será registrada en una bitácora en la que se especificará la cuenta de usuario, fecha, hora, registro modificado y modificación realizada. Lo anterior, tendrá como finalidad mantener un control y seguimiento de las acciones realizadas en los sistemas de información del SNI y del REPUVE.

El AAU contará con un módulo de reportes para la consulta de la información de las bitácoras de seguimiento a solicitud de los Enlaces Institucionales.

El AAU generará semestralmente un reporte del padrón de usuarios por entidad y lo enviará al CNI. Además, remitirá dicho padrón a cada institución con el fin de que sean validados por éstas. Lo anterior tiene el propósito de mantener el padrón de usuarios actualizado.

10. DE LA INTERPRETACIÓN Y CUMPLIMIENTO DE LOS PRESENTES LINEAMIENTOS

Corresponde al CNI interpretar el contenido de los Lineamientos a los que se refiere el presente Acuerdo para efectos administrativos, así como resolver aquellos casos no previstos en los mismos.

El CNI notificará por escrito las interpretaciones en el momento que fuera necesario, para una cooperación coordinada y comunicación efectiva con el AAU.

El CNI será el encargado de verificar el cumplimiento de los presentes Lineamientos. Su incumplimiento implicará responsabilidad jurídica conforme a lo dispuesto en la LGSNSP.

TRANSITORIOS

PRIMERO. El presente Acuerdo entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

SEGUNDO. Se deroga el Acuerdo de 2010 antes referido, así como todas aquellas disposiciones, normas, lineamientos, políticas, criterios y demás normatividad que se oponga a lo establecido en el presente Acuerdo.

Dado en la Ciudad de Villahermosa, Tabasco, a los 16 días del mes de diciembre de dos mil veintiuno.- El Titular del Centro Nacional de Información, **Jesús David Pérez Esparza**.- Rúbrica.