DOF: 20/04/2022

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.