

Acuerdo Ministerial No. 0555

María Paula Romo Rodríguez
MINISTRA DE GOBIERNO

CONSIDERANDO:

Que de acuerdo con el numeral 8 del artículo 3 de la Constitución de la República del Ecuador, es deber primordial del Estado ecuatoriano “Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción”;

Que el artículo 11 numeral 3 de la Constitución de la República del Ecuador, indica que: “*Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte. Para el ejercicio de los derechos y las garantías constitucionales no se exigirán condiciones o requisitos que no estén establecidos en la Constitución o la ley (...)*”;

Que el artículo 91 de la Constitución de la República del Ecuador, establece que: “La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna (...)”.

Que el artículo 92 ibídem dispone: “Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Así mismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas

CP
1



de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.”

Que el numeral 1 del artículo 154 de la mencionada Carta Magna establece a las y los ministros de Estado, además de las atribuciones establecidas en la ley: “1. Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión (...)”;

Que el artículo 163 de la misma Norma, dispone que “La Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional. Los miembros de la Policía Nacional tendrán una formación basada en derechos humanos, investigación especializada, prevención, control y prevención del delito y utilización de medios de disuasión y conciliación como alternativas al uso de la fuerza (...)”;

Que el artículo 226 de la Norma ibídem, consagra el principio de legalidad al siguiente tenor: “Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución”; y el artículo 227 ibídem establece los principios que rigen a “*La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación*”;

Que la Constitución de la República del Ecuador en su artículo 233 establece que, ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos. Además de que todo servidor público será sujeto a sanciones establecidas por delitos de peculado, cohecho, concusión y enriquecimiento ilícito;

Que el artículo 385 numeral 3 de la Constitución de la República del Ecuador, indica que: “*El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad (...) 3.*



Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir (...)”.

Que el artículo 416 de la Constitución de la República, dispone que las relaciones del Ecuador con la comunidad internacional responderán a los intereses del pueblo ecuatoriano, al que le rendirán cuenta sus responsables y ejecutores, y en consecuencia: “1. Proclama la independencia e igualdad jurídica de los Estados, la convivencia pacífica y la autodeterminación de los pueblos, así como la cooperación, la integración y la solidaridad (...)”;

Que el artículo 2 del Código Orgánico de Entidades de Seguridad Ciudadana y Orden Público, ordena que sus disposiciones son de aplicación obligatoria en todo el territorio nacional y se rigen al mismo, entre otras entidades la: “1. Policía Nacional (...)”;

Que el artículo 63 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público establece que el ministerio rector de la seguridad ciudadana, protección interna y orden público dirigirá las políticas, planificación, regulación, gestión y control de la Policía Nacional del Ecuador;

Que el artículo 64 del Código Orgánico de Entidades de Seguridad Ciudadana y Control de Orden Público, dispone las funciones del/la titular del ministerio rector de la seguridad ciudadana, protección interna y orden público, entre ellas: “4. Ejercer la representación legal, judicial y extrajudicial de la Policía Nacional;”;

Que el artículo 71 del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público establece: “*Organización.- Para el cumplimiento de las actividades de los subsistemas, la Policía Nacional se organiza por procesos y componentes jerárquicamente ordenados bajo los lineamientos y directrices del ministerio rector de la seguridad ciudadana, protección interna y orden público. Sin perjuicio de lo que se establezca en Reglamentos y estatutos internos, se determinan los siguientes procesos: 1. Gobernantes 2. Asesores o adjetivos; 3. Generadores de valor; y, 4. Desconcentrados. Los componentes son las unidades o instancias administrativas de la institución policial creados mediante acuerdo ministerial, según sus necesidades y requerimientos*”;

Que el artículo 23 inciso tercero de la Ley Orgánica de Seguridad Pública y del Estado referente a la seguridad ciudadana manifiesta: “*Se privilegiarán medidas preventivas y de servicio a la ciudadanía, registro y acceso a información, la ejecución de programas ciudadanos de prevención*

 3



del delito y de erradicación de violencia de cualquier tipo, mejora de la relación entre la policía y la comunidad, la provisión y medición de la calidad en cada uno de los servicios, mecanismos de vigilancia, auxilio y respuesta, equipamiento tecnológico que permita a las instituciones vigilar, controlar, auxiliar e investigar los eventos que se producen y que amenazan a la ciudadanía”;

Que el artículo 10 inciso segundo de la Ley Orgánica de Transparencia y Acceso a la Información Pública manifiesta que: *“Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública (...)”.*

Que el artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, establece que los ministros de Estado son competentes para el despacho de todos los asuntos inherentes a sus ministerios sin necesidad de autorización alguna del Presidente de la República;

Que mediante Decreto Ejecutivo No. 495 del 31 de agosto de 2018 publicado en el Registro Oficial 327 de 14 de septiembre de 2018, el licenciado Lenín Moreno Garcés, Presidente Constitucional de la República del Ecuador, designó como Ministra del Interior a la señora María Paula Romo Rodríguez;

Que mediante Decreto Ejecutivo No. 718 de 11 de abril de 2019, el licenciado Lenin Moreno Garcés, Presidente Constitucional de la República del Ecuador, en la Primera Disposición General señala: *“Una vez concluido el proceso de transformación institucional dispuesta en el presente Decreto Ejecutivo, en la normativa vigente en donde se haga referencia al “Ministerio del Interior” léase como “Ministerio de Gobierno”;*

Que el Acuerdo No. 039-CG de 13 de mayo de 2019 (Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos emitida por la Contraloría General del Estado, norma No. 410-01 denominada tecnología de la información, señala: *“Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional”.*



Que mediante Acuerdo Ministerial No. 011-2018, del 08 de agosto de 2018 publicado en el Registro Oficial 612 de 8 de noviembre de 2018, el Ministerio de Telecomunicaciones expide el Plan Nacional de Gobierno Electrónico 2018-2021, instrumento que muestra la situación actual del país en materia de gobierno electrónico, las acciones que serán ejecutadas en tres programas; y en el Capítulo 1 Fundamentos generales, numeral 5. Diagnóstico se establece que: *“Dentro de las iniciativas relevantes que ha implementado el gobierno en torno a la ciberseguridad se encuentra la implementación del Esquema Gubernamental de Seguridad de la Información - EGSi (...)”*;

Que el artículo 10 del Reglamento Sustitutivo de Seguridad de la Información, Buen Uso de Internet, Correo Electrónico, Control de los Recursos Informáticos y de Telecomunicaciones, establece que: “ Transmisión de datos.- A fin de garantizar la integridad y confidencialidad de la información y en razón de que los dispositivos móviles y los soportes extraíbles generan vulnerabilidades como divulgación no autorizada de datos, robo de datos, datos dañados o comprometidos, por la facilidad de uso, alta movilidad y capacidad de almacenamiento, la Dirección de Tecnología de Información y Comunicaciones, de forma programada y bajo pedido de las unidades administrativas (...)”;

Que en el informe Técnico de 09 de septiembre de 2019, suscrito por el Subsecretario de Estado - Gobierno Electrónico, se recomienda: *“Expedir mediante Acuerdo Ministerial el Esquema Gubernamental de Seguridad de la Información -EGSI-, debido a la necesidad de gestionar la seguridad de la información acorde a la evolución normativa y tecnológica, ya que actualmente los riesgos en seguridad muestran continuos cambios, se desarrollan nuevas amenazas y se revelan vulnerabilidades e incidentes de seguridad que tienen efectos considerables en la sociedad”*;

Que mediante Certificado No. QUI-048408, trámite No. 000776, de 25 de abril de 2016, la Dirección Nacional de Derechos de Autor y Derechos Conexos, del Instituto Ecuatoriano de la Propiedad Intelectual, inscribe como obra literaria de la Policía Nacional, Dirección Nacional de Comunicaciones al Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE – MÓVIL;

Que la Policía Nacional con el fin de atender la seguridad ciudadana y el orden público, ha desarrollado la herramienta tecnológica denominada Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, que constituye un medio esencial y fundamental de carácter estratégico, que integra, genera y articula la coordinación operativa y administrativa, por lo que es necesario normar su funcionamiento;

Gi
5



Que mediante Sentencia de la Corte Constitucional del Ecuador No. 55-14-JD/20, de 01 de julio de 2020, en el acápite 5 numeral cuarto, se dispone: *“El Ministerio de Gobierno, regule el funcionamiento del SIIPNE, emitiendo la normativa correspondiente en el plazo de seis meses, en la que deberá constar: la finalidad del SIIPNE, el contenido y origen de la información, usos y destinos, derechos de las personas a conocer sobre su información personal y mecanismos de actualización, rectificación, y eliminación o anulación de datos erróneos o que afecten derechos, garantías para la información confidencial y reservada, y responsabilidades usuarias del sistema por mal uso o violación a la confidencialidad y reserva.”*;

En ejercicio de las atribuciones que le confiere el artículo 154, numeral 1 de la Constitución de la República del Ecuador, en concordancia con el artículo 64 numeral 10, del Código Orgánico de las Entidades de Seguridad Ciudadana y Orden Público,

ACUERDA:

Expedir el presente

REGLAMENTO DEL SISTEMA INFORMÁTICO INTEGRADO DE LA POLICÍA NACIONAL DEL ECUADOR – SIIPNE

TÍTULO I

GENERALIDADES

CAPÍTULO I

OBJETO, ÁMBITO, FINALIDAD Y PRINCIPIOS

Artículo 1. Objeto.- El presente Reglamento tiene por objeto regular la estructura, funcionamiento y administración del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, estableciendo procedimientos para el acceso, uso, destino y manejo de la información; y, mecanismos de actualización, rectificación, eliminación y anulación de datos de forma segura cuando corresponda.

Artículo 2. Ámbito.- Las disposiciones del presente Reglamento son de cumplimiento, aplicación y observancia obligatoria para los usuarios del Sistema Informático Integrado de la Policía del Ecuador - SIIPNE, a nivel nacional; y, servidores policiales que se encuentren cumpliendo funciones en el exterior.



Artículo 3. Finalidad.- El Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE tiene por finalidad proporcionar información a través de la web y dispositivos móviles a los usuarios de los subsistemas, procesos y componentes de la Policía Nacional; para la ejecución de procesos operativos y de gestión institucional; y, brindar servicios a la comunidad, que contribuyen a la seguridad ciudadana y orden público.

Artículo 4. Principios.- El Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, se rige bajo los siguientes principios:

1. **Confidencialidad.-** La información almacenada en el sistema, es accesible únicamente a aquellos usuarios que están autorizados.
2. **Integridad.-** Los datos del sistema, deben permanecer de forma íntegra, como el generador de la información la originó, sin manipulaciones por terceros. Esto garantizará que la información no será modificada por usuarios no autorizados.
3. **Disponibilidad.-** La información del sistema, debe estar siempre disponible para su acceso y tratamiento por los usuarios que estén autorizados.
4. **Rectificabilidad.-** Los datos registrados en el sistema por las dependencias responsables de la administración de la información, son susceptibles de rectificación o supresión, en los casos y con los requisitos previstos en el presente reglamento.

CAPÍTULO II

DEFINICIONES

Artículo 5. Definiciones.- Para efectos de aplicación de este Reglamento, a continuación se establecen las siguientes definiciones:

1. **Actor.-** Es la entidad, dependencia o usuarios que interactúan en el sistema.
2. **Activos de información.-** Son los recursos tangibles e intangibles que utiliza el sistema para su funcionamiento.
3. **Amenaza.-** Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.


7



4. **Auditoría.-** Consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de Información salvaguarda el activo empresarial. Mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas.
5. **Automatizar.-** Es la transformación de tareas y actividades manuales a una automática, a través de herramientas de software.
6. **Base de datos.-** Es un conjunto de datos que permite guardar grandes cantidades de información de forma organizada.
7. **Código fuente.-** Son los archivos que contienen instrucciones para la correcta ejecución del sistema.
8. **Conectividad.-** Es la capacidad de establecer una conexión entre el sistema y dispositivos finales para el acceso a la información.
9. **Contingencia.-** Es un conjunto de procedimientos alternativos a la operatividad en procesos críticos, a fin de que continúen funcionando a pesar de una posible falla en los sistemas.
10. **Dato.-** Es la cifra, símbolo, letra o palabra que se ingresa al sistema para ser almacenada.
11. **Gestor Base de Datos.-** Es un sistema que permite crear, gestionar y administrar bases de datos de las plataformas tecnológicas.
12. **Hardware.-** Es la infraestructura tecnológica que permite la operatividad del sistema a través de elementos físicos.
13. **Información.-** Es el conjunto organizado de datos procesados manifestados a través de formas: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales y en medio, magnético, físico y electrónico.
14. **Integridad.-** La información del sistema deber ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.
15. **Perfil.-** Tipo de cuenta que un usuario tiene asignado en el sistema informático.
16. **Permiso.-** Facultad de realizar una tarea específica dentro de una aplicación del sistema.



17. **Pista de auditoría.-** Es el rastro de una transacción realizada por el usuario, en un sistema informático.
18. **Proceso.-** Es una secuencia de tareas, a fin de obtener un resultado específico.
19. **Procedimiento.-** Es una descripción detallada de cómo se debe llevar un proceso.
20. **Riesgo.-** Posibilidad que una amenaza pueda causar una pérdida o daño en un activo de información.
21. **Seguridad de la información.-** Conjunto de medidas preventivas y reactivas a adoptarse en los activos de información que permitan la preservación de la confidencialidad, integridad y disponibilidad de la información del sistema.
22. **Software.-** Es la parte intangible de componentes lógicos del sistema.
23. **Transacción.-** Es una interacción que realiza el usuario en el sistema.
24. **Trigger.-** Es un objeto asociado a tablas de un esquema de la base de datos, que se ejecuta cuando sucede alguna transacción, almacenándose en la base de datos.
25. **Usuarios.-** Es el conjunto de personas que, dependiendo del perfil de acceso al sistema, ejecutan tareas o actividades específicas.
26. **Versionamiento.-** Es el proceso de asignación de un nombre, código o número único, a un software para indicar su nivel de desarrollo.
27. **Vulnerabilidades.-** Debilidad de un activo de información que puede poner en peligro al sistema.

TÍTULO II

ESTRUCTURA DEL SISTEMA INFORMÁTICO INTEGRADO DE LA POLICÍA NACIONAL DEL ECUADOR – SIIPNE

CAPÍTULO I

SISTEMA INFORMÁTICO INTEGRADO DE LA POLICÍA NACIONAL DEL ECUADOR – SIIPNE

9



Artículo 6. Plataforma Tecnológica de la Policía Nacional.- Constituye el conjunto de sistemas, subsistemas de información y comunicación, que proporciona servicios tecnológicos a la institución; cuya administración y custodia es responsabilidad de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional del Ecuador.

Artículo 7. Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE.- Es una herramienta informática que almacena, procesa y custodia información proveniente de fuentes internas y externas, disponible a los usuarios de los subsistemas, procesos y componentes de gestión de la Policía Nacional para el desempeño de sus funciones.

El Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE forma parte de la plataforma tecnológica de la Institución; la información que provee es de uso exclusivo de los servidores de la institución policial, y está conformado por componentes, módulos y aplicaciones.

Artículo 8. Componentes del Sistema.- El Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, está conformado por los siguientes componentes:

1. Hardware.- Equipamiento de procesamiento, almacenamiento y periféricos, contenidos en el centro de datos institucional, que permiten la interacción del usuario con el sistema, y que está constituido por:

- a. Equipamiento de procesamiento y almacenamiento;
- b. Equipamiento de cableado estructurado;
- c. Equipamiento de seguridad informática; y.
- d. Infraestructura física y civil.

2. Software de Base.- Sistemas operativos utilizados para el funcionamiento, desarrollo e implementación del Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE.

3. Conectividad.- Medios de transmisión que establecen los enlaces de los operadores contratados, para exteriorizar los servicios, con la finalidad de que el usuario interactúe con el sistema.

4. Gestor de Base de Datos.- Sistemas estructurados que permiten administrar la información de las diferentes aplicaciones de las dependencias policiales, y que está constituido por:



a. Sistema de gestor de base de datos; y,

b. Sistema de gestor de auditorías.

5. Técnico Operacional.- Equipamiento que garantiza el funcionamiento y disponibilidad de los servicios del sistema, y que está constituido por:

a. Netwoking;

b. Energía;

c. Climatización; y,

d. Protecciones.

6. Información.- Activo de la Policía Nacional organizado y procesado por el Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, de uso exclusivo de la Policía Nacional para el cumplimiento de su misión constitucional, constituido por:

a. Fuentes Internas; y,

b. Fuentes Externas.

7. Usuarios.- Servidores de la institución policial que, dependiendo del perfil de acceso al Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, realizan y ejecutan múltiples operaciones, con distintos propósitos, y que son los siguientes:

a. Usuarios Privados; y,

b. Usuarios Públicos.

8. Módulo del Sistema.- Contenedor de aplicaciones desarrolladas para el manejo de la información de las dependencias policiales, que en conjunto conforman el Sistema Informático Integrado de la Policía Nacional del Ecuador, y que está constituido por:

a. Módulos de Gestión Administrativa;

b. Módulos de Gestión Operativa; y,

c. Módulos de Atención Ciudadana.

CGI

11



9. Aplicaciones.- Automatización de las tareas relacionadas a funciones específicas, acorde a los procesos y requerimientos de las dependencias policiales, según su gestión, que conforman los módulos del sistema.

Artículo 9. Creación de Módulos.- El módulo será creado a solicitud de la dependencia policial requirente, por la gestión encargada de las tecnologías de la información y comunicación.

El módulo deberá agrupar aplicaciones con un mismo objetivo y naturaleza organizacional, su denominativo estará acorde a su gestión misional.

Artículo 10. Desarrollo de Aplicaciones.- La programación y diseño de las aplicaciones será de responsabilidad de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional, acorde a los requerimientos de las dependencias policiales.

La creación de las aplicaciones deberá utilizar buenas prácticas de desarrollo seguro, para mantener la seguridad en las diferentes etapas del ciclo de vida del software.

Artículo 11. Implementación de Aplicaciones.- Es la ejecución o puesta en marcha de las nuevas aplicaciones y/o actualizaciones en el ambiente de producción, luego de su validación y aceptación por las dependencias policiales requirentes.

Artículo 12. Mantenimiento Evolutivo de Aplicaciones.- Es la reprogramación o rediseño de una aplicación en producción, a petición de la dependencia requirente o por eventos detectados por la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional.

Si la reprogramación o rediseño causa un impacto alto a la funcionalidad o estructura de la aplicación, será considerado como un nuevo desarrollo, para lo cual deberá cumplir el procedimiento previsto en el presente reglamento.

TÍTULO III

FUENTES DE INFORMACIÓN DEL SISTEMA

CAPÍTULO I

FUENTES INTERNAS Y EXTERNAS

Artículo 13. Origen de la Información.- El Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, consume, genera, comparte e intercambia datos e información de fuentes



- b. Registro de nómina;
 - c. Registro de vivienda fiscal;
 - d. Registro académico de los servidores policiales;
 - e. Registro de emergencia sanitaria;
 - f. Registro de la administración de equipamiento logístico, bienes muebles e inmuebles, armas y pertrechos;
 - g. Registro del manejo de la identidad institucional;
 - h. Registro del cumplimiento de recomendaciones por parte de los órganos de control del Estado;
 - i. Registro de conducta policial;
 - j. Registro de casos; y,
 - k. Registro de sumarios administrativos.
3. Otra información que generen las dependencias de la Policía Nacional, para el cumplimiento de sus funciones.

Artículo 16.- Información personal sobre detenciones.- La Policía Nacional registra únicamente información personal respecto de detenciones de ciudadanos en los casos previstos en la ley. Este tipo de información es de carácter confidencial, y solo podrán acceder a ella su titular y los demás actores autorizados en el presente reglamento.

Artículo 17.- Fuentes Externas.- Son las instituciones públicas y/o privadas que proveen información para el consumo de los usuarios en el Sistema Informático Integrado de la Policía Nacional – SIIPNE.

La información proporcionada al sistema por instituciones públicas y privadas, se constituye en una fuente de consulta en apoyo a las operaciones policiales. Esta información proviene de las siguientes instituciones:

- a. **Registro Civil.-** Datos de identificación de personas, direcciones domiciliarias;



- b. **Agencia Nacional de Tránsito.-** Tipo de licencia, restricciones de vehículos, situación o identificación vehicular;
- c. **Consejo de la Judicatura.-** Boletas de apremio, boletas de captura, boletas de detención, situación o estado judicial;
- d. **Fiscalía General del Estado.-** Retenciones y liberaciones vehiculares y otras. La información proporcionada por la Fiscalía General del Estado es entregada en formato físico para registro en el sistema por parte de los usuarios autorizados.
- e. **Servicio de Rentas Internas.-** Información tributaria;
- f. **Subsecretaría de Migración del Ministerio de Gobierno.-** Ingreso y salida de personas extranjeras;
- g. **Interpol.-** Alertas de difusión internacional para las policías que forman parte de la Interpol, con el objeto cumplir con las disposiciones de la autoridad competente; y,
- h. **Otros.-** Información proporcionada por otras instituciones con las que la Policía Nacional del Ecuador establezca convenios interinstitucionales, para el cumplimiento de su misión constitucional.

CAPÍTULO II

USO Y DESTINO DE LA INFORMACIÓN DEL SISTEMA INFORMÁTICO INTEGRADO DE LA POLICÍA NACIONAL - SIIPNE

Artículo 18. Uso de la Información. – La información de las fuentes internas y externas del sistema, serán utilizados por los servidores de la institución policial únicamente cuando se encuentren de servicio, en los siguientes casos:

1. Trámites Administrativos Institucionales;
2. Operativos Policiales;
3. Investigaciones Judiciales; y,
4. Cumplimiento de disposiciones de Autoridad Competente.

Artículo 19. Destino de la Información.- La información contenida en el sistema será destinada exclusivamente para los servidores de la institución policial, en cumplimiento de su cargo y función, en irrestricto respeto a los derechos y garantías de las personas.

El módulo de servicios a la ciudadanía cuenta con aplicaciones en las cuales los usuarios registran información para un uso específico; sin acceso a la información de fuentes internas o externas definidas en este reglamento.

Artículo 20. Uso Indebido de la Información.- Los usuarios autorizados y/o terceras personas que hagan mal uso de la información contenida en el sistema, serán responsables de sus actuaciones y serán sancionadas administrativa, civil y penalmente por las autoridades competentes, de conformidad con el ordenamiento jurídico vigente.

Se considerará uso indebido de la información del sistema en los siguientes casos:

1. Compartir usuarios y claves de acceso de uso personal con terceras personas;
2. Otorgar privilegios a usuarios, que no estén acorde a su cargo o función;
3. Realizar consultas a los módulos del sistema ajenas a las funciones que desempeña;
4. Crear usuarios y claves de acceso a personas no autorizadas;
5. Divulgar la información contenida en el sistema a personas no autorizadas;
6. Modificar, alterar, marginar y/o eliminar información del sistema sin autorización;
7. Obtener réditos económicos o de cualquier otra naturaleza por proporcionar información a terceros; y,
8. Hacer uso del sistema sin encontrarse de servicio;
9. Las demás que vulneren los derechos y garantías de las personas.

TÍTULO IV

ACTORES Y ADMINISTRACIÓN DEL SISTEMA INFORMÁTICO INTEGRADO DE LA POLICÍA NACIONAL DEL ECUADOR-SIIPNE

CAPÍTULO I



ACTORES DEL SISTEMA

Artículo 21. Actores del Sistema.- Son las partes que interactúan en el Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, estos son:

1. La gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional;
2. Las dependencias responsables de la administración de la información; y,
3. Los usuarios del sistema.

Artículo 22. La Gestión Encargada de las Tecnologías de la Información y Comunicación de la Policía Nacional.- Es el responsable de la administración técnica del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE.

Artículo 23. Atribuciones y Responsabilidades.- Son atribuciones y responsabilidades de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional, a través de sus departamentos, las siguientes:

1. Mantener la operatividad y disponibilidad del sistema;
2. Automatizar procesos e implementar los requerimientos de las dependencias policiales requirentes en el sistema;
3. Definir la metodología de intercambio y consumo de información del sistema, entre las dependencias de la Policía Nacional y otras instituciones públicas, privadas, nacionales e internacionales;
4. Definir y gestionar el Sistema Gestor de Base de Datos, que utilizará la plataforma tecnológica institucional;
5. Asesorar en la suscripción de convenios entre instituciones para el consumo y entrega de información, buscando el mejoramiento continuo del sistema;
6. Asesorar y coordinar la suscripción de acuerdos a nivel institucional para el consumo y entrega de información, buscando el mejoramiento continuo del sistema;
7. Definir y aplicar la metodología y arquitectura en el desarrollo del sistema;

CS
17



8. Gestionar el módulo Administración del Sistema;
9. Gestionar la modernización permanente de los sistemas, hardware, software del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, acorde a la evolución de las tecnologías de la información y comunicación;
10. Implementar controles de seguridad, con el fin de conservar la disponibilidad, integridad y confidencialidad de la información custodiada en el sistema;
11. Asesorar para el mejoramiento y desarrollo del sistema;
12. Definir e implementar niveles de seguridad;
13. Implementar en el sistema los requerimientos de seguridad definidos por los propietarios de la información;
14. Automatizar, actualizar e implementar nuevas funcionalidades en el sistema;
15. Cambiar el estado de las cuentas de usuarios para administradores;
16. Cambiar el estado de las cuentas de usuarios subadministradores, a pedido de las dependencias responsables de la administración de la información;
17. Atender los requerimientos de las entidades policiales respecto a los pedidos de la autoridad competente, para la entrega de información de transacciones realizadas en el Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE;
18. Implementar aplicaciones para la generación de reportes no considerados en el requerimiento inicial por las dependencias generadoras de la información; a fin de evitar conexiones directas con el gestor de base de datos;
19. Custodiar el código fuente del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE; y,
20. Las demás atribuciones y responsabilidades establecidas en la normativa vigente, en el ámbito de su competencia.



Artículo 24. Dependencias responsables de la administración de la Información.- Son las responsables de los módulos y la información que generan y consultan; ejecutando procesos y procedimientos establecidos, acorde a sus funciones.

Artículo 25. Atribuciones y Responsabilidades.- Son atribuciones y responsabilidades de las dependencias responsables de la administración de la información las siguientes:

1. Mantener procesos y procedimientos actualizados y validados;
2. Gestionar la suscripción de convenios entre instituciones para el consumo y entrega de información, en coordinación con la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional;
3. Establecer acuerdos para compartir información, entre dependencias policiales;
4. Solicitar a la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional, la automatización de los procesos de la dependencia policial a ser implementado en el sistema;
5. Determinar los lineamientos para el respaldo, resguardo y conservación de la información;
6. Determinar los permisos de acceso a la información contenida en su módulo, acorde a los procesos internos;
7. Definir controles para modificar y eliminar registros de sus aplicaciones;
8. Solicitar la implementación de seguridades, de acuerdo a la normativa técnica y legal vigente, para la clasificación de la información;
9. Validar la automatización de los procesos, previo a la suscripción del acta de aceptación del sistema;
10. Nombrar servidores policiales en servicio activo como subadministrador para la gestión del módulo a su cargo;
11. Elaborar procedimientos e instructivos de uso del módulo a su cargo;
12. Valorar el tipo de eliminación de información que requieran sus procesos de acuerdo a la normativa legal vigente; y,



13. Las demás atribuciones y responsabilidades establecidas en la normativa vigente, en el ámbito de su competencia.

Artículo 26. Usuarios del Sistema. - Son las personas que teniendo o no una cuenta de usuario hacen uso del sistema.

CAPÍTULO II

USUARIOS DEL SISTEMA

Artículo 27. Tipos de Usuario. - El Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, tendrá dos tipos de usuario:

1. **Usuario Privado.** - Es el servidor policial o civil que labora en la Policía Nacional, que posee una cuenta con credenciales de acceso al sistema, para el ingreso a los módulos y aplicaciones privadas.
2. **Usuario Público.** - Es la persona que no requiere de una cuenta de usuario para el ingreso únicamente a las aplicaciones del sistema que la Policía Nacional brinda como un servicio a la ciudadanía.

Artículo 28. Creación de Usuarios del Sistema.- Dentro del Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, existen dos formas para crear usuarios:

1. Registro Personal; y,
2. Registro a través de un Subadministrador.

Artículo 29. Registro Personal.- El servidor policial desde el momento que es dado el alta como miembro de la institución policial, ingresará y se registrará como usuario del sistema.

Artículo 30. Registro a través del Subadministrador.- La dependencia policial requirente, solicitará al subadministrador del módulo administración, el registro y creación de usuarios para servidores policiales y empleados civiles que laboran en la institución policial, siempre que cumplan los requisitos establecidos en el presente reglamento.

Artículo 31. Cuentas de Usuario. – Es el registro mediante el cual se asigna un nombre de usuario único y una contraseña para acceder al Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE.



Artículo 32. Perfiles de los Usuarios.- Para la administración y acceso al Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, existen cuentas de usuarios con diferentes perfiles y tipos de permiso, determinados por la función asignada.

De acuerdo al perfil y tipo de permiso se clasifican en:

1. Administrador;
2. Administrador SIIPNE;
3. Subadministrador; y,
4. Usuario.

Artículo 33. Administrador.- Es el perfil asignado a un usuario que tendrá la facultad de crear administradores SIIPNE.

Artículo 34. Requisitos para ser Administrador.- Para ser designado administrador debe cumplir los siguientes requisitos:

1. Pertenecer orgánicamente a la dependencia policial encargada de la gestión de las tecnologías de la información y comunicación de la Policía Nacional;
2. Ser designado de manera formal por parte de la máxima autoridad de la dependencia policial encargada de la gestión de las tecnologías de la información y comunicación de la Policía Nacional;
3. Suscribir acuerdo de confidencialidad; y,
4. Poseer título de tercer nivel en materias afines a las tecnologías de la información y comunicación.

Artículo 35. Atribuciones y Responsabilidades.- Son atribuciones y responsabilidades del administrador las siguientes:

1. Activar y desactivar el perfil de administrador SIIPNE, previo al cumplimiento de los requisitos establecidos en el presente reglamento;
2. Mantener un archivo actualizado y documentos de respaldo de la activación y desactivación de los registros de administradores SIIPNE;

Así
21



3. Llevar el registro actualizado de los administradores SIIPNE;
4. Informar a la máxima autoridad de la gestión encargada de las tecnologías de la información y comunicación, el traslado, vacaciones, descanso médico y cese de funciones, para que se proceda a su inmediata desactivación en el sistema;
5. Brindar la inducción al nuevo administrador respecto a las atribuciones y responsabilidades de su competencia;
6. Suscribir las actas de relevo de funciones de administrador cuando sea dado el traslado y/o cese de funciones; y,
7. Cumplir con las obligaciones establecidas en el acuerdo de confidencialidad.

Artículo 36. Administrador SIIPNE.- Es el perfil asignado al usuario en el Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, que le permite gestionar los procesos y procedimientos de manera general del módulo a su cargo.

Artículo 37. Requisitos del Administrador SIIPNE.- Para ser designado como administrador SIIPNE, deberá cumplir los siguientes requisitos:

1. Pertenecer al orgánico de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional;
2. Ser designado de manera formal por parte de la máxima autoridad de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional;
3. Suscribir acuerdo de confidencialidad; y,
4. Poseer título de tercer nivel en materias afines a las tecnologías de la información y comunicación.

Artículo 38. Atribuciones y Responsabilidades.- Son atribuciones y responsabilidades del administrador SIIPNE las siguientes:

1. Activar y desactivar el perfil de subadministrador, conforme la solicitud de la dependencia responsable del módulo, previo al cumplimiento de los requisitos establecidos en el presente reglamento;



2. Mantener un archivo actualizado y documentos de respaldo de la activación y desactivación de los subadministradores;
3. Llevar el registro actualizado de los subadministradores;
4. Informar a la máxima autoridad de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional, el traslado, vacaciones, descanso médico y cese de funciones, para que se proceda a su inmediata desactivación en el sistema;
5. Brindar soporte a los subadministradores del módulo asignado al servicio y/o dependencia policial;
6. Brindar la inducción al nuevo administrador SIIPNE, respecto a las atribuciones y responsabilidades de su competencia;
7. Suscribir las actas de relevo de funciones de administrador SIIPNE cuando sea dado el traslado y/o cese de funciones; y,
8. Cumplir con las obligaciones establecidas en el acuerdo de confidencialidad.

Artículo 39. Subadministrador.- Es el perfil asignado a un usuario en el sistema, encargado de otorgar acceso a los usuarios en el módulo y aplicaciones bajo su responsabilidad.

Artículo 40. Requisitos para ser Subadministrador.- Son requisitos para ser designado subadministrador los siguientes:

1. Pertenecer al orgánico de la dependencia policial responsable de la subadministración del módulo;
2. Ser servidor policial directivo y/o técnico operativo en servicio activo;
3. Ser nombrado de manera formal por parte de la máxima autoridad de la dependencia policial responsable de la subadministración del módulo;
4. Suscribir acuerdo de confidencialidad; y,
5. Tener conocimientos en materias afines a tecnologías de la información y comunicación, debidamente acreditado.

OS
23



Artículo 41. Atribuciones y Responsabilidades.- Son atribuciones y responsabilidades del subadministrador las siguientes:

1. Activar y desactivar el perfil y tipo de acceso al usuario en el módulo y aplicaciones, acorde a su función; previa autorización de la máxima autoridad de la dependencia policial;
2. Crear, actualizar y eliminar los catálogos y configuraciones de las aplicaciones del sistema que requieran, previa autorización de la máxima autoridad de la dependencia requirente;
3. Revisar el cumplimiento de los requisitos establecidos en el presente reglamento, para la activación y desactivación de usuarios;
4. Elaborar y actualizar los manuales de los procesos de los módulos y aplicaciones;
5. Mantener un archivo actualizado y documentos de respaldo de la activación, desactivación y permisos asignados a los usuarios;
6. Brindar soporte de funcionalidad a los usuarios del módulo asignado;
7. Realizar la inducción del manejo de las aplicaciones asignadas a los usuarios del sistema;
8. Suscribir las actas de relevo de funciones de subadministrador cuando sea dado el traslado, vacaciones, licencias o cese de funciones, previa notificación a la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional;
9. Cumplir con las obligaciones establecidas en el acuerdo de confidencialidad;
10. Conocer el funcionamiento del módulo y aplicaciones, según el ámbito de su competencia;
11. Gestionar nuevos requerimientos y la desactivación de las aplicaciones que dejaron de ser funcionales para la dependencia policial, previa la respectiva justificación y autorización de la máxima autoridad de la misma;
12. Solicitar información de auditorías a la máxima autoridad de la dependencia policial, de las cuentas de los usuarios, respecto a las transacciones realizadas desde las aplicaciones funcionales del sistema, cuando así lo requiera o exista presunciones de mal uso; información que debe ser canalizada por la gestión encargada de las tecnologías de la información y comunicación; y,
13. Cumplir con las demás atribuciones legales, conforme a sus competencias.



Artículo 42. Usuario.- Es el perfil asignado a una persona que tiene permisos para el uso del sistema de acuerdo a su función.

Artículo 43. Requisitos para ser Usuario.- Para ser usuario del sistema deberá cumplir los siguientes requisitos:

1. Prestar servicios en la dependencia policial propietaria del módulo;
2. Suscribir acuerdo de confidencialidad; y,
3. Tener conocimientos básicos en el manejo de herramientas informáticas.

Artículo 44. Atribuciones y Responsabilidades.- Son atribuciones y responsabilidades del usuario las siguientes:

1. Solicitar la habilitación de permisos de acceso al módulo a la máxima autoridad de la dependencia policial;
2. Insertar, consultar, modificar y eliminar información de acuerdo a su cargo o función y perfil;
3. Informar al subadministrador el traslado, vacaciones, descanso médico y cese de funciones, para que se proceda a su inmediata desactivación en el sistema;
4. Suscribir las actas de relevo de funciones de usuario cuando sea dado el traslado y/o cese de funciones, mismas que serán puestas en conocimiento de la máxima autoridad de la dependencia policial;
5. Cumplir con las obligaciones establecidas en el acuerdo de confidencialidad;
6. Mantener la reserva de su usuario y contraseña; y,
7. Cumplir con las demás atribuciones legales, conforme a sus competencias.

TÍTULO V

PERMISOS DE LOS USUARIOS Y DERECHOS DE LAS PERSONAS SOBRE LA INFORMACIÓN DEL SISTEMA

CAPÍTULO I

PERMISOS DE LOS USUARIOS EN EL SISTEMA

25



Artículo 45. Permisos de los Usuarios.- Es la facultad que otorgan los subadministradores de los módulos a los usuarios de las aplicaciones, de acuerdo al cargo o función, para realizar operaciones específicas de la información generada por fuentes internas en las aplicaciones de los módulos del Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, estos son:

1. **Insertar.-** Es el ingreso de información en las aplicaciones de sus módulos de los procedimientos administrativos y operativos; procede de oficio, por orden de autoridad competente y a petición de la persona interesada.

2. **Modificar.-** Es el cambio o actualización de la información que realiza el usuario autorizado en la aplicación, procede de oficio, por orden de autoridad competente y a petición de la persona interesada.

3. **Eliminar.-** Es el borrado de la información almacenada de la dependencia responsable de la administración de la información en el sistema; procederá únicamente de oficio y con orden de autoridad competente.

La gestión encargada de las tecnologías de la información y comunicación, por ningún motivo eliminará información directamente en la base de datos del Sistema Informático Integrado de la Policía Nacional del Ecuador– SIIPNE.

4. **Consultar.-** Es la búsqueda y visualización de la información que contiene el sistema de acuerdo al parámetro de búsqueda, ingresada por el usuario autorizado; procede de oficio, por orden de autoridad competente y a petición de la persona interesada.

5. **Margar.-** Es la modificación del estado del registro de información a través de la aplicación respectiva, la información marginada no podrá ser visualizada por los usuarios; sin embargo, seguirá almacenada en la base de datos, procede por orden de autoridad competente y a petición de la persona interesada.

6. **Transferir.-** Consiste en el traspaso de datos de un registro de detención policial de una persona a otra, cuando se verifica la suplantación de identidad, persona no identificada o la existencia de homónimos, procede por orden de autoridad competente y por petición de la persona interesada.

El permiso de transferencia se otorgará únicamente al usuario autorizado de la aplicación de registro de detención policial del módulo Policía Judicial.



Artículo 46. Procedencia de la ejecución de cambios.- Los usuarios autorizados de las aplicaciones de los módulos de acuerdo a su cargo y función, podrán ejecutar los permisos sobre la información contenida en el sistema en los siguientes casos:

1. De Oficio.- Las dependencias de la Policía Nacional por medio del usuario autorizado, en cumplimiento de sus funciones, sin necesidad de petición de la parte interesada o por orden de autoridad competente, ejecutará los permisos sobre la información contenida en el sistema.

Cuando el ingreso de la información sea de oficio, se cumplirá el siguiente procedimiento:

- a. Generación de la necesidad de ejecutar los permisos dentro del sistema por parte del usuario autorizado o de la dependencia policial responsable de la administración de la información;
- b. Verificación de los datos en el sistema, por parte del usuario autorizado;
- c. La máxima autoridad administrativa de la dependencia policial responsable de la administración de la información, dispondrá la ejecución de los permisos, según sea el caso; y,
- d. Ejecución de los permisos en el sistema por parte del usuario autorizado.

2. Por Orden de Autoridad Competente.- Cuando una autoridad judicial, fiscal o administrativa emite una orden expresa para que la Policía Nacional proceda a ejecutar los permisos que constan en el sistema.

Cuando la disposición proceda de autoridad competente, se cumplirá el siguiente procedimiento:

- a. Recepción de la documentación que contenga la orden de la autoridad competente, la cual deberá constar en original o copia certificada;
- b. La máxima autoridad administrativa de la dependencia policial responsable de la administración de la información, dispondrá el cumplimiento de la orden de autoridad competente;
- c. Ejecución de la disposición por parte del usuario autorizado en el sistema; y,
- d. Notificación a la autoridad del cumplimiento de la disposición.

3. A petición de la persona interesada.- Cuando la persona titular de la información respecto de la cual hubiese uno o más datos errados, solicita a la dependencia propietaria de la información la ejecución de los permisos sobre su información personal generada en el sistema.

27



Cuando la solicitud proceda a petición de la persona interesada, se cumplirá el siguiente procedimiento:

- a. Presentación de la solicitud por parte del titular de la información o su representante legal, en la cual deberá constar un correo electrónico, y número telefónico para la notificación, adjuntando:
 1. La copia de la cédula de ciudadanía o documento de identificación del titular y en el caso del representante legal deberá además adjuntar la documentación que lo acredite;
 2. La documentación o declaración que justifique la petición en originales o copias certificadas.
- b. Recepción de la solicitud;
- c. Verificación de la información por parte del usuario autorizado;
- d. Informe jurídico sobre la información cuyo error se reclama, que será remitido a la máxima autoridad de la dependencia policial responsable de la administración de la información;
- e. Autorización de la máxima autoridad de la dependencia policial responsable de la administración de la información;
- f. Ejecución de la disposición por parte del usuario autorizado en el sistema; y,
- g. Notificación al peticionario.

La administración sustanciará y ejecutará los permisos de insertar, modificar, eliminar, consultar, marginar y transferir información, de la forma más eficiente y en el menor tiempo posible, sin afectar la calidad de su gestión.

Las notificaciones a la autoridad competente y a petición de la persona interesada se realizarán dentro de las 48 horas de ejecutado la disposición o solicitud.

En los casos de petición de la persona interesada, no se requerirá abogado patrocinador.

Artículo 47. Registros de información de fuentes externas.- La información de las fuentes externas no será objeto de cambio o alteración, por cuanto la Policía Nacional únicamente utiliza sus bases de datos como fuente consulta.

CAPÍTULO II



DERECHOS Y GARANTÍAS DE LOS CIUDADANOS RESPECTO DE LA INFORMACIÓN PERSONAL EN EL SISTEMA

Artículo 48. Información de Carácter Personal.- Las personas que consideren afectado su derecho a la protección de datos personales u otros conexos, por errores, inconsistencias o datos incompletos contenidos en la información de carácter personal y confidencial que almacena el sistema, respeto del registro de detenciones de los ciudadanos, podrán solicitar inserción, modificación, eliminación, marginación, transferencia o realizar consultas respecto de dicha información, según corresponda, de acuerdo a lo establecido en este reglamento.

En la solicitud y trámite de cualquiera de estas acciones, las y los servidores policiales observarán siempre todos los derechos y garantías de las personas.

Artículo 49. Aplicativo Antecedentes Policiales.- Es el aplicativo en el cual se registra las detenciones de las personas aprehendidas en delito flagrante, o por orden de autoridad competente; situaciones legales que poseen permisos para insertar, modificar, eliminar, consultar, marginar y transferir información.

Estos permisos se ejecutarán previo el cumplimiento de los requisitos y procedimientos establecidos en el capítulo anterior del presente reglamento.

Artículo 50. Insertar.- Procede la inserción cuando la información existente en el sistema es incompleta, esta acción se realizará:

1. De oficio;
2. Por orden de autoridad competente; y,
3. A petición de la persona interesada.

Artículo 51. Modificar.- Procede la modificación, cambio y/o corrección por un error o actualización de la información constante en el proceso de registro de detención, esta acción se realizará:

1. De oficio;
2. Por orden de autoridad competente; y,
3. A petición de la persona interesada.

CS
29



Artículo 52. Eliminar.- Procede la eliminación de toda la información constante en el registro de antecedentes policiales, esta acción se realizará:

1. Por orden de autoridad competente; y,
2. A petición de la persona interesada.

En los siguientes casos:

- a. Por resolución judicial en caso de sobreseimiento, debidamente ejecutoriado; y,
- b. Por sentencia absolutoria o ratificatoria del estado de inocencia, debidamente ejecutoriada;

Artículo 53. Consultar.- Procede la verificación de información en el sistema para dar cumplimiento de las disposiciones de autoridad competente, esta acción se realizará:

1. De oficio;
2. Por orden de autoridad competente; y,
3. A petición de la persona interesada.

En los casos que la consulta sea solicitada a petición de la persona interesada, el titular de la información o su representante legal debidamente autorizado deberá llenar el formulario respectivo.

Artículo 54. Marginar.- Es un trámite que tiene como finalidad marginar el registro de detención personal de ciudadanos que mantienen un registro activo en el Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, como efecto de una detención o por una acción penal que se haya iniciado en su contra.

Procede la marginación de toda la información constante en el registro de antecedentes policiales, esta acción se realizará:

1. Por orden de autoridad competente; y,
2. A petición de persona interesada.

La marginación de los registros de detención personales procede en los siguientes casos:

- a. Sobreseimiento;



- b. Prescripción de la acción;
- c. Prescripción de la pena;
- d. Extinción de la acción;
- e. Sentencia absolutoria o ratificatoria del estado de inocencia;
- f. Acuerdo conciliatorio con la resolución de archivo definitivo;
- g. Desestimación y archivo;
- h. Por amnistía;
- i. Por Indulto;
- j. Sentencia condenatoria con la certificación del cumplimiento de la pena; y,
- k. Otros que den por finalizado el proceso penal, debidamente ejecutoriados.

En los casos que la marginación sea solicitada a petición de la persona interesada, esta deberá llenar el formulario de solicitud de marginación de la información adjuntando los siguientes documentos:

1. Copia debidamente certificada de la resolución judicial ejecutoriada o del documento que sustente la solicitud de marginación, según el caso;
2. Copia certificada de la boleta de excarcelación, cuando corresponda; y,
3. Copia de la cédula de ciudadanía o documento de identidad.

Artículo 55. Transferir.- Procede el traspaso de datos de un registro de detención policial de una persona a otra, cuando se verifica la suplantación de identidad, persona no identificada o la existencia de homónimos, esta acción se realizará:

1. Por orden de autoridad competente; y,
2. A petición de la persona interesada.

En los casos de registros que, por encontrarse incompletos o cuya información sea ambigua y respecto de los cuales el sistema no permita su transferencia, se procederá con su eliminación total.

TÍTULO VI

SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA

CAPÍTULO I

SEGURIDAD DE LA INFORMACIÓN

Artículo 56. Seguridad de la Información.- La información que se encuentra en el Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, está protegida por una infraestructura tecnológica de seguridad y una arquitectura de software, para evitar la materialización de posibles amenazas y garantizar la disponibilidad, integridad y confidencialidad de la información del sistema, la misma que será objeto de auditoría, de acuerdo a los procesos establecidos por la institución y de conformidad con la normativa legal vigente.

Todo incidente de seguridad de la información, deberá ser puesto en conocimiento del Comité de Seguridad de la Información de la Policía Nacional.

Artículo 57. Gestión de los Activos de Información.- El Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, para la gestión de los activos de información poseerá controles implementados en el sistema, basados en los procedimientos establecidos por las dependencias policiales propietarias de los módulos, para la administración e identificación de los activos de información de conformidad con la normativa legal vigente.

Artículo 58. Acceso al Sistema.- El acceso al sistema y a la información, se controla a través de la verificación y autenticación de credenciales del usuario, acorde a los perfiles y permisos asignados, de acuerdo al cargo o función que desempeña.

Artículo 59. Acceso a la Información.- La información que se encuentra contenida en los módulos y aplicativos privados del Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, no es de libre acceso y será de uso exclusivo de la Policía Nacional y de las instituciones con las cuales se establezca un acceso a la información de acuerdo a los convenios suscritos.

Artículo 60. Acceso al Código Fuente del Sistema.- El acceso al código fuente del sistema por seguridad es restringida, mediante controles técnicos y administrativos.

Artículo 61. Encriptación.- El sistema utiliza métodos de encriptación en las credenciales del usuario y en la información determinada por las dependencias policiales; así como, en los procesos



de transferencia de datos y respaldos de la información, para proteger la confidencialidad, integridad, disponibilidad y autenticidad de la información contenida y gestionada en el Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE.

Los métodos de encriptación los establecerá la gestión encargada de las tecnologías de la información y comunicación de la institución.

Artículo 62. Seguridad Física.- Comprende los controles implementados para la protección de los perímetros de las instalaciones en donde se aloja la infraestructura tecnológica del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, que procesa, almacena y custodia la información.

En caso de desastres naturales, ataques maliciosos o accidentes, la gestión encargada o de las tecnologías de la información y comunicación ejecutará los planes de contingencia elaborados para el efecto.

Artículo 63. Seguridad de las Operaciones.- Son los procedimientos y controles establecidos e implementados por la gestión encargada de las tecnologías de la información y comunicación, Comité de Seguridad de la Información y demás entes de control, para la gestión de capacidad, separación de ambientes y copias de seguridad, a fin de garantizar la disponibilidad y funcionamiento del Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE.

Artículo 64. Acuerdo de Confidencialidad.- Es un instrumento jurídico que tiene por objeto proteger la información que almacena y administra el Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE, de conformidad con las normas legales vigentes.

Todos los usuarios que tienen acceso al sistema, deberán suscribir el acuerdo de confidencialidad, para evitar la divulgación, mal uso o violación a la confidencialidad y reserva de la información.

El acuerdo de confidencialidad establece de derechos y obligaciones, sanciones, vigencia y notificaciones, a las que se sujetan los usuarios del sistema.

El acuerdo de confidencialidad será suscrito por los usuarios del sistema, como uno de los requisitos para la utilización de los módulos del Sistema Informático Integrado de la Policía Nacional del Ecuador – SIIPNE.

CAPÍTULO II

33



RESPALDO Y MONITOREO DE LA INFORMACIÓN

Artículo 65. Respaldo de la Información.- La gestión encargada de las tecnologías de la información y comunicación, realizará respaldos de seguridad de la información contenida en el Sistema Informático Integrado de la Policía Nacional - SIIPNE; para lo cual, establecerá con las dependencias responsables de la administración de la información, el periodo de tiempo de conservación de los respaldos, de acuerdo a su importancia; en observancia de la normativa legal vigente.

Artículo 66. Copias de los Archivos de Configuración.- La gestión encargada de las tecnologías de la información y comunicación, realizará las copias de los archivos de configuración del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, con base al procedimiento que permita garantizar la continuidad y disponibilidad del sistema; en observancia de la normativa legal vigente.

Artículo 67. Monitoreo.- La gestión encargada de las tecnologías de la información y comunicación, realizará el monitoreo del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE y la infraestructura que forma parte de la Plataforma Tecnológica de la Policía Nacional, para garantizar su operatividad y disponibilidad.

Artículo 68. Vulnerabilidades Técnicas.- Son debilidades o deficiencias de seguridad del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE y la infraestructura que forma parte de la Plataforma Tecnológica de la Policía Nacional, que podrían afectar su funcionamiento al materializarse la amenaza.

Artículo 69. Seguridad en el Desarrollo y Mantenimiento del Sistema.- La seguridad forma parte integral del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, a lo largo de todo el ciclo de vida del sistema, documentando las etapas de: levantamiento de requerimientos, análisis, diseño, desarrollo, prueba, implementación y mantenimiento, mediante la aplicación de normas de desarrollo de software seguro.

Las actualizaciones y nuevas funcionalidades del sistema, solicitados por parte de los propietarios de la información, se realizan a través de procedimientos formales, y con un sistema de versionamiento y control administrativo.



Artículo 70. Incidentes de Seguridad de la Información del Sistema.- La gestión encargada de las tecnologías de la información y comunicación, elaborará y ejecutará procedimientos de atención, registro, análisis, evaluación, seguimiento y respuesta, a los incidentes de seguridad.

Artículo 71. Continuidad del Sistema. - Son las medidas adoptadas para garantizar la operatividad y funcionalidad del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, ante eventos adversos y antrópicos.

La gestión encargada de las tecnologías de la información y comunicación conjuntamente con el Comité de Seguridad de la Información de la Policía Nacional, elaborarán e implementarán el Plan de Continuidad del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE; en observancia de la normativa técnica aplicable.

TÍTULO VII

CONTROL Y EVALUACIÓN AL SISTEMA INFORMÁTICO INTEGRADO DE LA POLICÍA NACIONAL DEL ECUADOR - SIIPNE

Artículo 72. Controles del Sistema.- Son los procesos informáticos desarrollados, implementados y controlados por la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional, respecto a los requerimientos solicitados por las dependencias responsables de la administración de la información.

Artículo 73. Trazabilidad de Transacciones.- Es el control implementado por la gestión de las tecnologías de la información y comunicación, al esquema del Sistema Informático Integrado de la Policía Nacional - SIIPNE, a través de disparadores automáticos (triggers) y visualizados en el sistema.

Artículo 74. Evaluación del Sistema.- La evaluación de los controles y procedimientos de seguridad de la información del sistema, será dispuesta por el Comité de Seguridad de la Información Institucional; a través de una planificación establecida para el efecto, esta evaluación se basará en lineamientos, estándares y normativas relacionadas con la seguridad de la información.

Artículo 75. Auditorías del Sistema.- La gestión encargada de las tecnologías de la información y comunicación mantiene una planificación de auditorías para detectar riesgos e implementar seguridades en el Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, con la finalidad de conservar la confidencialidad, integridad y disponibilidad de la información.

OC
35



DISPOSICIONES GENERALES

Disposición General Primera.- Las dependencias responsables de la administración de la información en coordinación con la dependencia encargada de las tecnologías de la información y comunicación, el Comité de Seguridad de la Información de la Policía Nacional y el Oficial de Seguridad de la Información, establecerán mecanismos de control y seguridad de la información en el Sistema Informático Integrado de la Policía Nacional - SIIPNE.

Disposición General Segunda.- Las dependencias responsables de la administración de la información, definirán en el requerimiento de sus procesos a la gestión encargada de las tecnologías de la información y comunicación, el tipo de eliminación de la información que utilizarán las aplicaciones, ya sean físicas o lógicas.

Disposición General Tercera.- La priorización de la automatización de los requerimientos de las dependencias responsables de la administración de la información en el Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, serán valorados de acuerdo al procedimiento establecido por la gestión encargada de las tecnologías de la información y comunicación, conforme la Política Tecnológica Institucional.

Disposición General Cuarta.- La propiedad intelectual y los derechos sobre el desarrollo de software implementado por los servidores policiales y/o civiles en el desempeño de su cargo o función, corresponderá a la Policía Nacional del Ecuador. El código fuente no será utilizado por otras dependencias policiales, instituciones públicas o privadas sin la autorización de la gestión encargada de las tecnologías de la información y comunicación de la Policía Nacional.

Disposición General Quinta.- La incorporación de nuevos módulos al Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, se realizará por necesidad de las dependencias policiales o innovación tecnológica, cumpliendo con los controles y procesos establecidos en el presente reglamento.

DISPOSICIONES TRANSITORIAS

Disposición Transitoria Primera.- Las dependencias externas e internas que generen y procesen información de origen policial a través de sistemas y/o aplicaciones tecnológicas, en el plazo de un año contado desde la vigencia del presente reglamento, se integrarán a la Plataforma Tecnológica de la Policía Nacional, de acuerdo a la Política Tecnológica Institucional.



Disposición Transitoria Segunda.- Las dependencias responsables de la administración de la información, en el plazo de seis meses contados desde la vigencia del presente reglamento, deberán definir y establecer los controles que tendrán sus respectivos módulos y aplicaciones, para asegurar los activos de información.

Disposición Transitoria Tercera.- La gestión encargada de las tecnologías de la información y comunicación, en coordinación con la gestión de planificación y gestión estratégica y las dependencias generadoras de la información de la Policía Nacional en el plazo un año contado desde la vigencia del presente reglamento elaborarán los manuales, procedimientos e instructivos necesarios para el cumplimiento del presente reglamento.

Disposición Transitoria Cuarta.- Las dependencias responsables de la administración de la información, que posean aplicaciones en los sistemas SIIPNE Fase I y SIIPNE Fase II, migrarán su información a la versión del sistema en vigencia en el plazo máximo de seis meses contados desde la vigencia del presente reglamento.

DISPOSICIONES FINALES

Disposición Final Primera. - El presente Reglamento del Sistema Informático Integrado de la Policía Nacional del Ecuador - SIIPNE, entrará en vigencia a partir de la fecha de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Disposición Final Segunda. – Encárguese la ejecución del presente reglamento al Viceministerio de Gobierno a través de la Policía Nacional.

COMUNÍQUESE Y PUBLÍQUESE.-

Dado en el Despacho de la Ministra de Gobierno, en Quito DM, el 13 de noviembre del 2020.


María Paula Romo Rodríguez
MINISTRA DE GOBIERNO