

RESOLUCIÓN NRO. 003-NG-DINARP-2022

LA DIRECTORA NACIONAL DE REGISTROS PÚBLICOS

CONSIDERANDO:

- Que,** el numeral 2 del artículo 16 de la Constitución de la República del Ecuador, dispone: *“Todas las personas, en forma individual o colectiva, tienen derecho a: (...) 2. El acceso universal a las tecnologías de información y comunicación (...);”*
- Que,** el numeral 2 del artículo 17 de la Constitución de la República del Ecuador, ordena: *“El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: (...) 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada (...);”*
- Que,** el numeral 19 del artículo 66 de la Constitución de la República del Ecuador, manda: *“Se reconoce y garantizará a las personas: (...) 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (...);”*
- Que,** el artículo 226 de la Constitución de la República del Ecuador, establece: *“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”;*
- Que,** el artículo 227 de la Constitución de la República del Ecuador, preceptúa: *“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,** el artículo 1 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, señala: *“Principio de Publicidad de la Información Pública. - El acceso a la información pública es un derecho de las personas que garantiza el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las*

instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley”;

Que, el literal d) del artículo 2 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, establece: *“La presente Ley garantiza y norma el ejercicio del derecho fundamental de las personas a la información conforma las garantías consagradas en la Constitución Política de la República, Pacto Internacional de Derechos Civil y Políticos, Convención Interamericana sobre Derechos Humanos y demás instrumentos internacionales vigentes, de los cuales nuestro país es signatario. Persigue los siguientes objetivos: (...) d) Garantizar la protección de la información personal en poder del sector público y/o privado”;*

Que, el artículo 1 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, dispone: *“Esta Ley tiene por objeto disponer la optimización de trámites administrativos, regular su simplificación y reducir sus costos de gestión, con el fin de facilitar la relación entre las y los administrados y la Administración Pública y entre las entidades que la componen; así como, garantizar el derecho de las personas a contar con una Administración Pública eficiente, eficaz, transparente y de calidad”;*

Que, el artículo 2 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, determina: *“Las disposiciones de esta Ley son aplicables a todos los trámites administrativos que se gestionen en:*

- 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral, Transparencia y Control Social, en la Procuraduría General del Estado y la Corte Constitucional;*
- 2. Las entidades que integran el régimen autónomo descentralizado y regímenes especiales;*
- 3. Las empresas públicas;*
- 4. Las entidades que tienen a su cargo la seguridad social;*
- 5. Las entidades que comprenden el sector financiero público;*
- 6. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado;*
- 7. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados y regímenes especiales para la prestación de servicios públicos; y,*
- 8. Las personas naturales o jurídicas del sector privado que sean gestoras delegadas o concesionarias de servicios públicos.*

Asimismo, el contenido de la presente Ley es aplicable a las relaciones que se generen a partir de la gestión de trámites administrativos entre el Estado y las y los administrados; entre las entidades que conforman el sector público; y entre éstas y las y los servidores públicos.

Las disposiciones de esta Ley serán aplicables a las demás entidades del sector privado que tengan a su cargo trámites ciudadanos solo en los casos en que esta Ley lo establezca expresamente.

Esta Ley no es aplicable a los trámites administrativos del sector defensa o que comprometan la seguridad nacional”;

- Que,** los numerales 4 y 7 del artículo 3 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, recogen los principios de “*Tecnologías de la información*” e “*Interoperabilidad*”, en función de los cuales las entidades reguladas por dicha norma harán uso de tecnologías de la información y comunicación con el fin de mejorar la calidad de los servicios públicos y optimizar la gestión de trámites administrativos; así como, intercambiar información mediante el uso de medios electrónicos y automatizados, para la adecuada gestión de los trámites administrativos;
- Que,** los numerales 4 y 5 del artículo 8 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, ordenan: “*La simplificación de trámites a cargo de las entidades reguladas por esta Ley deberá estar orientada a: (...) 4. La implementación del uso progresivo, continuo y obligatorio de herramientas tecnológicas. 5. La incorporación de controles automatizados que minimicen la necesidad de estructuras de supervisión y control adicionales (...)*”;
- Que,** el artículo 15 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, preceptúa: “*Trámites en línea. - Las entidades reguladas por esta Ley que cuenten con trámites administrativos que se puedan generar en línea, deben garantizar que el trámite, en su totalidad, se pueda realizar en línea y no podrán exigir la presentación del original o copia del comprobante de la gestión de dicho trámite como requisitos para finalizar el mismo.*

Cuando el trámite administrativo se pueda gestionar en línea, las entidades reguladas por esta Ley no podrán exigir la presencia física de la o el interesado”;

Que, los numerales 4 y 5 del artículo 18 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, establecen: *“Obligaciones de las Entidades Públicas. - Las entidades reguladas por esta Ley deberán cumplir, al menos, con las siguientes obligaciones: (...) 4. Implementar mecanismos, de preferencia electrónicos, que permitan conocer, en cualquier momento, el estado de los trámites de las y los interesados. 5. Implementar mecanismos, de preferencia electrónicos, para la gestión de trámites administrativos, tales como la firma electrónica y cualquier otro que haga más eficiente la Administración Pública”;*

Que, el artículo 21 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, expresa: *“Del uso obligatorio de los datos del Sistema Nacional de Registros Públicos. - Sin perjuicio de lo establecido en la Ley del Sistema Nacional de Registro de Datos Públicos, todas las entidades reguladas por esta Ley deberán utilizar obligatoriamente la información que reposa en:*

- 1. Sus propias bases de datos, alimentadas por información proporcionada por el propio ciudadano o por terceros, con anterioridad a la fecha del trámite; y*
- 2. El Sistema Nacional de Registros Públicos, para lo cual deberán cumplir con el trámite establecido en la ley que lo regula y demás normativa pertinente. Para el efecto, dichas entidades tienen la obligación de integrar los registros y bases de datos que estén a su cargo al Sistema Nacional de Registro de Datos Públicos en el plazo y con las formalidades requeridas por la Ley del Sistema Nacional de Registro de Datos Públicos y la entidad que presida el Sistema Nacional de Registro de Datos Públicos”;*

Que, el artículo 24 Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, indica: *“La identidad de las personas naturales se demostrará con la presentación de la cédula de identidad o ciudadanía, el documento nacional de identidad, el pasaporte o la licencia de conducir, indistintamente. En caso de que las entidades implementen mecanismos de autenticación biométrica u otros similares para demostrar la identidad, ya no será necesaria la presentación de ninguno de los documentos referidos en el inciso anterior (...);”*

Que, el artículo 25 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, determina: *“La identificación de las personas jurídicas se acreditará con la presentación del Registro Único del Contribuyente otorgado por el Servicio de Rentas Internas. Sin perjuicio de lo expuesto en el inciso anterior, si para el trámite administrativo se requiere, además, conocer la identidad del representante legal de la persona jurídica, las entidades reguladas por esta Ley deberán solicitar la presentación de uno de los documentos establecidos en el artículo precedente, y constatar la calidad de representante legal accediendo al sistema informático de cualquiera de los entes encargados de su registro. Para el efecto, los nombramientos de representantes legales de personas jurídicas deben ser registrados obligatoriamente en las entidades pertinentes conforme la ley, las que deberán mantener actualizada su base de datos y prestar todas las facilidades para que las demás entidades accedan a dicha información”;*

Que, el artículo 31 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos,

establece: *“El ente rector de telecomunicaciones, gobierno electrónico y sociedad de la información tendrá competencia para ejercer la rectoría, emitir políticas, lineamientos, regulaciones y metodologías orientadas a la simplificación, optimización y eficiencia de los trámites administrativos, así como, a reducir la complejidad administrativa y los costos relacionados con dichos trámites; y controlar su cumplimiento”.*

Que, el numeral 1 del artículo 32 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, preceptúa: *“La entidad rectora de simplificación de trámites tendrá las siguientes atribuciones: 1. Emitir políticas públicas, lineamientos, metodologías, regulaciones y realizar estudios técnicos para la simplificación, optimización y eficiencia de trámites administrativos y controlar su cumplimiento (...);”*

Que, el artículo 1 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, establece: *“La presente ley crea y regula el sistema de registros públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros. El objeto de la ley es: garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías”;*

Que, el artículo 2 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, dispone: *“La presente Ley rige para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos”;*

Que, el artículo 30 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, manda: *“Créase la Dirección Nacional de Registros Públicos, como organismo de derecho público, con personería jurídica, autonomía administrativa, técnica, operativa, financiera y presupuestaria, adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información. Su máxima autoridad y representante legal será la Directora o Director Nacional, designada o designado por la Ministra o Ministro (...);”*

Que, los numerales 1 y 2 del artículo 31 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, establece que la Dirección Nacional de Registros Públicos tendrá, entre otras, las siguientes atribuciones y facultades: *“1. Presidir el Sistema Nacional de Registros Públicos, cumpliendo y haciendo cumplir sus finalidades y objetivos; 2. Dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema (...);”*

Que, el artículo 13 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, señala: *“Firma electrónica. - Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba*

y reconoce la información contenida en el mensaje de datos”;

Que, el artículo 20 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, determina: *“Certificado de firma electrónica. - Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad”;*

Que, el artículo 7 del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, ordena: *“Dirección Nacional de Registros Públicos. - Es la entidad que preside el Sistema Nacional de Registros Públicos, responsable de la gestión, administración y cumplimiento de sus objetivos. Para el cumplimiento de sus fines, goza de autonomía administrativa, técnica, operativa y financiera. (...)”;*

Que, las Normas de Control Interno para la Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos, dentro de la Norma 410 “Tecnología de la Información”, la 410-04 Políticas y procedimientos, determinan: *“La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.*

La Unidad de Tecnología de Información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales, además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Se implantarán procedimientos de supervisión de las funciones de tecnología de información,

ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos”;

Que, el Ministro de Telecomunicaciones y de la Sociedad de la Información, a través del Oficio Nro. MINTEL-MINTEL-2020-0183-O, de 26 de mayo de 2020, dispone: “(...) *Considerando que es necesario que el Estado cree un sistema de autenticación único, que brinde un mecanismo confiable para el acceso a diferentes portales institucionales, para lo cual es necesario recopilar información personal para el enrolamiento y posterior autenticación de sus usuarios, configurándose dicho sistema como un repositorio que deberá agregarse al SINARDAP.*

En función de los antecedentes citados, es indispensable implementar mecanismos electrónicos que faciliten la interacción entre el ciudadano y la administración pública, unificando los mecanismos de acceso de la ciudadanía a los servicios y trámites en línea que atiende el sector público, por lo cual se solicita a la Dirección Nacional de Registro de Datos Públicos la implementación y soporte del Sistema de Autenticación Única para las plataformas de las entidades que forman parte de SINARDAP. (...)

La DINARDAP deberá garantizar la disponibilidad del Sistema de Autenticación Única, dimensionando su uso para todo ciudadano que requiera activar un usuario para proceder a los trámites y servicios del Estado (...);

Que, mediante Acuerdo Ministerial Nro. MINTEL-MINTEL-2021-0003, de 22 de junio de 2021, la doctora Vianna Di Maino Isaías, Ministra de Telecomunicaciones y de la Sociedad de la Información, resuelve: “(...) *Designar a la abogada Angie Karina Jijón Mancheno como Directora Nacional de Registros Públicos, quién ejercerá las competencias y atribuciones previstas en la Ley y Orgánica del Sistema Nacional de Registros Públicos y demás normativa aplicable (...);*

En ejercicio de las facultades que le otorga la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos y su Reglamento de aplicación,

RESUELVE:

EXPEDIR LA NORMA DE FUNCIONAMIENTO DEL SISTEMA DE AUTENTICACIÓN ÚNICA (SAU)

CAPÍTULO I GENERALIDADES

Art. 1. Ámbito de aplicación. - Esta norma es de aplicación obligatoria para la Entidad Administradora del Sistema de Autenticación Única (SAU), personas naturales, Instituciones públicas, privadas o mixtas

que se enrolen al sistema, teniendo acceso a los servicios y trámites gubernamentales en línea en interoperabilidad, y servicios propios de la Dirección Nacional de Registros Públicos DINARP.

Art. 2. Objeto. - Establecer medios de enrolamiento al Sistema de Autenticación Única (SAU) en beneficio de las personas naturales, Instituciones públicas, privadas o mixtas, con el fin de contar con un mecanismo unificado de autenticación único de identidad para dicho proceso en el Sistema y, por ende, tener acceso a diferentes servicios integrados.

Art. 3. Sistema de Autenticación Única "SAU". - El Sistema de Autenticación Única (SAU), es un sistema integral de autenticación, autorización y registro único para el acceso seguro a servicios electrónicos gubernamentales integrados para el ciudadano y servidores públicos, a través de un único usuario y contraseña.

Art. 4. Finalidades del Sistema de Autenticación Única (SAU). - El Sistema de Autenticación Única (SAU), tiene por finalidad:

1. Promover la creación y utilización de una credencial digital de acceso única a los portales de servicios y sistemas gubernamentales, facilitando la prestación de servicios públicos, acceso a la información; y, garantizando la protección de datos de carácter personal.
2. Crear condiciones de confianza en la ciudadanía para el uso de medios electrónicos, estableciendo las medidas necesarias para la protección de sus derechos fundamentales, en especial aquellos relacionados con la intimidad y la no divulgación de datos de carácter personal, a través de estrictos procesos de enrolamiento, autenticación, acceso y registro de eventos.
3. Proveer a los usuarios formas de autenticación y acceso seguro a su información personal, así como, a los servicios y trámites en línea activados de Instituciones públicas.
4. Simplificar procedimientos administrativos de las instituciones públicas, contribuyendo en la mejora operativa del Sistema Nacional de Registros Públicos, incrementando la eficacia y la eficiencia en procesos de autenticación, autorización y registro de eventos, mediante el uso de las tecnologías de la información con garantías técnicas y legales.
5. Unificar en un solo repositorio de datos, la información para la autenticación y registro de acceso de los usuarios en los diferentes servicios y trámites en línea implementados por las instituciones públicas; y, activos en el Sistema. Con excepción de aquellos usuarios que cuenten con credenciales del servicio de Dato Seguro V1.0.

Art. 5. Glosario de Términos. - Para efectos de la presente Resolución, se definen los siguientes términos:

- a. Autenticación: Método de acreditación o confirmación de una determinada identidad en medios electrónicos.
- b. Autorización: Proceso que determina a qué recursos de un sistema el usuario autenticado podrá acceder.

- c. Credenciales: Herramienta de acreditación tecnológica compuesta por usuario y clave, registrados en instituciones públicas para el acceso a servicios en línea.
- d. Dirección de Protocolo de Internet "IP": Es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo de comunicaciones.
- e. Enrolamiento: Procedimiento mediante el cual las personas se vinculan al Sistema de Autenticación Única (SAU).
- f. Fedatario Administrativo: Es la persona delegada por la Institución fuente, encargada de validar la identidad del usuario en el proceso de enrolamiento.
- g. Firma Electrónica: Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.
- h. Instituciones fuente: Instituciones públicas, privadas o mixtas integradas al Sistema Nacional de Registros Públicos, que activen trámites ciudadanos en línea.
- i. Medios electrónicos: Cualquier mecanismo, equipamiento o sistema que permite producir, almacenar o transmitir información digital.
- j. Manual de Procedimiento Técnico de Integración al Sistema de Autenticación Única (SAU): Documento guía para llevar a cabo el procedimiento de integración de Instituciones al Sistema de Autenticación Única (SAU).
- k. Manual de Procedimiento de Uso del Sistema de Autenticación Única (SAU): Documento guía para llevar a cabo la operación cotidiana del Sistema de Autenticación Única (SAU).
- l. Reconocimiento facial: Metodología de identificación o verificación a través de una imagen, video o cualquier elemento audiovisual del rostro de un sujeto.
- m. Repositorio de Datos: Archivo centralizado donde se almacena y mantiene información digital.
- n. Trámite en línea: Acción o conjunto de acciones direccionadas a lograr un beneficio o cumplir una obligación.
- o. SAU: Sistema de Autenticación Única
- p. Validación presencial: Consiste en acudir de forma física ante un Fedatario Administrativo para que confirme la identidad de una persona en el procedimiento de enrolamiento al Sistema de Autenticación Única (SAU).
- q. Validación telemática: Consiste en la confirmación de la identidad de una persona a través de medio tecnológicos:
 - I. Videoconferencia: Consiste en una videoconferencia entre el Fedatario Administrativo designado por la institución fuente y la persona en proceso de enrolamiento;
 - II. Video pregrabado: Consiste en enviar al correo electrónico autorizado de la Institución fuente, un video pre grabado que cumpla con las directrices establecidas en el Manual de Procedimiento Técnico de Integración SAU.
- r. Usuario: Persona natural o jurídica que cumpla con el proceso de enrolamiento en el Sistema de Autenticación Única (SAU).

Art. 6. Entidad Administradora del Sistema de Autenticación Única (SAU). - La Dirección Nacional de Registros Públicos o quien haga sus veces, será la entidad encargada de la administración del Sistema de Autenticación Única (SAU).

Art. 7. Atribuciones y responsabilidades de la Entidad Administradora del Sistema de Autenticación Única (SAU). - Son obligaciones de la Entidad Administradora del Sistema de Autenticación Única (SAU), las siguientes:

- a Cumplir y hacer cumplir la Constitución de la República del Ecuador, la Ley y la presente Resolución;
- b Mantener confidencialidad y resguardo de los datos personales de acceso al Sistema de Autenticación Única (SAU);
- c Facilitar el acceso al Sistema de Autenticación Única (SAU) a los usuarios e Instituciones integradas;
- d Permitir al usuario actualizar los datos de registro proporcionados posteriormente a su enrolamiento al Sistema de Autenticación Única (SAU);
- e Facilitar el restablecimiento de las contraseñas a los usuarios del Sistema de Autenticación Única (SAU);
- f Emitir y/o reformar los manuales que considere necesarios para el correcto uso e implementación del Sistema de Autenticación Única (SAU); y,
- g Presentar informes y/o reportes sobre el Sistema Único de Autenticación (SAU) al Ministerio de Telecomunicaciones y de la Sociedad de la Información o quien haga sus veces; cuando éste así lo requiera.

Art. 8. Instituciones integradas al Sistema de Autenticación Única (SAU). - Son aquellas entidades establecidas en el artículo 2 de la Ley para la Optimización y Eficiencia de Trámites Administrativos, que cuenten con servicios y trámites administrativos que se puedan gestionar en línea, y que hayan cumplido con el procedimiento de integración al Sistema de Autenticación Única (SAU).

Art. 9. Responsabilidad de las Instituciones integradas al Sistema de Autenticación Única (SAU). - Las Instituciones integradas al Sistema de Autenticación Única (SAU), son las únicas responsables del contenido de su información proyectada en el sistema, en los servicios y trámites en línea que presten; así como, en los límites para su acceso.

Art. 10. Del Coordinador SINARP. - El Coordinador SINARP designado, será el contacto oficial entre la Institución integrada y la Entidad Administradora del Sistema de Autenticación Única (SAU).

Las Instituciones que requieran hacer uso del Sistema de Autenticación Única (SAU), deberán, a través de su Coordinador SINARP, crear, eliminar, modificar y asignar los roles en el Sistema de Autenticación Única (SAU).

Corresponderá al Coordinador SINARP, ejercer las facultades, atribuciones y responsabilidades establecidas en la presente norma y las demás emitidas por la Dirección Nacional de Registros Públicos.

En caso de cambio de Coordinador SINARP, la Institución integrada y el Coordinador SINARP deberán cumplir con el procedimiento establecido en la normativa legal

Art. 11. Atribuciones y responsabilidades del Coordinador SINARP. - El Coordinador SINARP, tendrá las siguientes atribuciones y responsabilidades:

- a. Coordinar y solicitar la asignación de su rol dentro de la plataforma del Sistema de Autenticación Única (SAU); y, en el caso de que exista un cambio de Coordinador SINARP dentro de la Institución, solicitar la eliminación del anterior rol; así como coordinar y requerir la asignación de su rol, conforme se detalla en los manuales respectivos;
- b. Administrar los roles y canalizar la integración de las aplicaciones de la Institución integrada a la que pertenece en el Sistema de Autenticación Única (SAU);
- c. Llevar un control sistemático de la utilización de la plataforma del Sistema de Autenticación Única (SAU), conforme los parámetros que para el efecto haya establecido la Entidad Administradora del Sistema de Autenticación Única (SAU);
- d. Controlar y supervisar el buen uso y funcionamiento del Sistema de Autenticación Única (SAU);
- e. Gestionar oportunamente las necesidades para el uso de los servicios del Sistema de Autenticación Única (SAU) de la Institución integrada a la que pertenece, conservando un expediente con toda la documentación gestionada para el uso de la herramienta;
- f. En caso de detectar un mal uso del Sistema de Autenticación Única (SAU) o ataques cibernéticos, deberá notificar de manera inmediata de este particular a su máxima autoridad, y a la Entidad Administradora del Sistema de Autenticación Única (SAU), para que se inicien las acciones administrativas y legales pertinentes;
- g. Notificar y solicitar la depuración a la DINARP de la base de Fedatarios asignados conforme la necesidad institucional.

Art. 12. Obligaciones de los usuarios del Sistema de Autenticación Única (SAU). - Los usuarios del Sistema de Autenticación Única (SAU), tienen las siguientes obligaciones:

- a. Proporcionar información veraz y precisa que se requiera para el proceso de enrolamiento. La responsabilidad sobre la veracidad y autenticidad de los datos registrados es de exclusiva responsabilidad de la o el declarante, tanto en el momento de registro, como en el uso;
- b. Realizar el enrolamiento de sus datos para obtener las credenciales de acceso;
- c. Mantener actualizada su información en el Sistema de Autenticación Única (SAU). El administrador del Sistema de Autenticación Única (SAU) no asumirá responsabilidad alguna derivada de la falta de actualización de la información del usuario, y;
- d. Utilizar con fines legítimos la información y datos a los que tengan acceso a través del Sistema de Autenticación Única (SAU). El uso indebido de esa información acarreará las responsabilidades administrativas, civiles y penales que correspondan.

Art. 13. De las credenciales. - Las credenciales de acceso generadas por los usuarios son de uso personal e intransferible, en virtud de lo cual, el usuario será el único responsable de su custodia e utilización.

CAPÍTULO II

DE LOS PROCESOS DE ENROLAMIENTO, AUTENTICACIÓN Y REGISTRO DE EVENTOS EN EL SISTEMA DE AUTENTICACIÓN ÚNICA

Art. 14. Del enrolamiento. - El procedimiento de enrolamiento al Sistema de Autenticación Única (SAU), se lo deberá realizar por una única vez, a través de cualquier Institución integrada, conforme lo establecido en el Manual de Procedimiento de Uso emitido por la Entidad Administradora.

Art. 15. De la validación de la identidad en el enrolamiento. - Con la finalidad de confirmar su identidad en el enrolamiento al Sistema de Autenticación Única (SAU), el usuario que realiza el procedimiento, contará con las siguientes opciones:

- a. Validación a través de reconocimiento facial;
- b. Validación a través de firma electrónica;
- c. Validación ante Fedatario Administrativo:
 1. Presencial; o,
 2. Por medios telemáticos:
 - 2.1. Videoconferencia
 - 2.2. Video pre grabado
- d. Validación por medio de credenciales de instituciones públicas integradas al Sistema de Autenticación Única (SAU).

Art. 16. Validación a través de reconocimiento facial. - Se validará la identidad del usuario a través del software automatizado de identificación biométrica, capaz de identificar a una persona o de comprobar su identidad mediante la comparación y el análisis de los modelos, formas y proporciones de sus rasgos y contornos faciales.

Art. 17. Validación a través de firma electrónica. - Se validará la identidad del usuario a través del certificado de firma electrónica, el cual legitima la vinculación de una persona determinada.

Art. 18. Validación ante un Fedatario Administrativo. - El Fedatario Administrativo es el contacto oficial entre la Institución integrada y el usuario en enrolamiento, quien constatará la identidad del usuario, a través de los canales presenciales o telemáticos habilitados, debiendo hacer uso del Sistema de Autenticación Única (SAU); y, en el caso necesario, del aplicativo "Ficha Simplificada" para la constatación de información del usuario en proceso de enrolamiento.

Art. 19. De las atribuciones y responsabilidades del Fedatario Administrativo. - Los Fedatarios Administrativos tendrán las siguientes atribuciones y responsabilidades:

- a. Cumplir con el proceso de asignación de su rol dentro del Sistema de Autenticación Única (SAU), y solicitar la eliminación del mismo conforme se detalla en los manuales respectivos;
- b. Constatar la identidad de los usuarios que requieran enrolarse al Sistema de Autenticación Única (SAU);
- c. Gestionar oportunamente el requerimiento del usuario;
- d. Hacer uso de los medios tecnológicos para la validación de usuarios por medios telemáticos;
- e. Hacer buen uso del Sistema de Autenticación Única (SAU), en cumplimiento de sus funciones; y,
- f. Ejecutar sus funciones con eficacia, eficiencia, calidad y celeridad.

Art. 20. Validación por medio de credenciales de Instituciones públicas integradas al Sistema de Autenticación Única (SAU). - Se podrá validar la identidad del usuario con al menos una credencial habilitada en Instituciones públicas integradas al Sistema de Autenticación Única (SAU).

Art. 21. De la excepción al enrolamiento. - Los usuarios que cuenten con credenciales de acceso a Dato Seguro V1.0, estarán enrolados automáticamente al Sistema de Autenticación Única (SAU).

Art. 22. De la autenticación. - Culminado el procedimiento de enrolamiento, el usuario contará con las credenciales generadas por el Sistema de Autenticación Única (SAU), que servirán para la autenticación de su identidad cuando acceda a los servicios y trámites en línea habilitados por las Instituciones integradas al sistema.

Art. 23. Del registro de eventos. - Las autenticaciones generadas cada vez que los usuarios hagan uso del Sistema de Autenticación Única (SAU), se registrarán en el Sistema, debiendo contar con la siguiente información: fecha, hora, dirección IP a través de la cual se efectuó el ingreso, y los demás datos de acceso que sean definidos en el "Manual de Procedimiento de Uso del Sistema de Autenticación Única (SAU)".

Esta información deberá ser conservada por la Entidad Administradora durante siete (7) años, de conformidad a lo establecido en la Ley Orgánica de la Contraloría General del Estado.

El registro de eventos dispuesto en el presente artículo, tiene como finalidad mantener disponible y ordenada la información que permita demostrar o acreditar información de eventos, si así lo requiere una autoridad competente.

Art. 24. Inactividad. – La Entidad Administradora, podrá de oficio inactivar una cuenta, cuando el usuario durante el plazo de dos (2) años no acceda a los servicios y trámites en línea de las Instituciones Integradas al Sistema de Autenticación Única (SAU). La inactividad de la cuenta de un usuario, impedirá

el acceso electrónico a los servicios prestados por las Instituciones que integran el Sistema de Autenticación Única (SAU).

Art. 25. Reactivación. - En caso de que la cuenta de un usuario sea declarada inactiva y este último desee reactivarla, deberá solicitar la reactivación a la Entidad Administradora del Sistema de Autenticación Única (SAU), cumpliendo con el procedimiento establecido para el efecto.

Art. 26. Deshabilitación. - Si una cuenta es deshabilitada, los usuarios no podrán acceder al Sistema de Autenticación Única (SAU) de forma definitiva. Las cuentas de los usuarios se deshabilitarán por las siguientes causales:

- a. A petición de parte; y,
- b. De oficio:
 - i. Por denuncia de una posible suplantación de identidad;
 - ii. Por notificación de cambio de representante legal tratándose de personas jurídicas, en cuyo caso, el nuevo representante legal deberá iniciar el procedimiento de enrolamiento.

En caso de que una cuenta sea deshabilitada, la persona natural o jurídica, deberá iniciar el procedimiento de enrolamiento nuevamente.

DISPOSICIONES GENERALES

PRIMERA. - El cumplimiento de la presente Resolución, estará sujeto al procedimiento de vigilancia y control a ser ejercido por la Dirección Nacional de Registros Públicos, conforme a lo dispuesto en los numerales 1 y 2 del artículo 31 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos.

SEGUNDA. - Encárguese la ejecución, cumplimiento y seguimiento de la presente Resolución a la Coordinación de Gestión Registro y Seguimiento y la Coordinación de Infraestructura y Seguridad Informática de la Dirección Nacional de Registros Públicos.

TERCERA. - Encárguese a la Dirección de Comunicación Social, la difusión y publicación de la presente Resolución en la página web Institucional.

DISPOSICIONES TRANSITORIAS

PRIMERA. - Dispóngase a la Coordinación de Gestión, Control y Seguimiento de la DINARP, promover la integración al Sistema de Autenticación Única (SAU) a las Instituciones detalladas en el artículo 2 de la Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos.

SEGUNDA. - En el término no mayor de diez (10) días, contados a partir de la vigencia de la presente Resolución, la Coordinación de Gestión, Registro y Seguimiento, deberá entregar el caso de negocio con las mejoras a realizar en la Plataforma Sistema de Autenticación Única (SAU).

TERCERA. - En el término no mayor de quince (15) días, contados a partir de la entrega del caso de negocio, la Coordinación de Infraestructura y Seguridad Informática, deberá realizar las modificaciones técnicas y tecnológicas necesarias al Sistema de Autenticación Única (SAU), para el estricto cumplimiento de la presente Resolución, sin perjuicio de que el Sistema empiece a operar bajo las condiciones técnicas y operativas existentes.

Una vez las Instituciones integradas al Sistema de Autenticación Única (SAU), hayan cumplido con lo establecido en la Disposición Transitoria Séptima, la Coordinación de Infraestructura y Seguridad Informática, en el término de ochenta (80) días deberá incorporar como método de autenticación del Sistema de Autenticación Única (SAU), la validación a través de credenciales de Instituciones públicas.

CUARTA. - En el término de diez (10) días, contados a partir de la vigencia de la presente Resolución, la Coordinación de Infraestructura y Seguridad Informática deberá conectar las credenciales de acceso a Dato Seguro a las del Sistema de Autenticación Única (SAU).

QUINTA. - En el término no mayor de quince (15) días, contados a partir de las acciones de mejora, la Coordinación de Infraestructura y Seguridad Informática y la Coordinación de Gestión, Registro y Seguimiento deberán reformar el *“Manual de Procedimiento Técnico de Integración del Sistema de Autenticación Única (SAU)”* y *“Manual de Procedimiento de Uso del Sistema de Autenticación Única (SAU)”*, respectivamente.

SEXTA. - Las Instituciones integradas al Sistema de Autenticación Única (SAU), en el término de dos (2) días, contados a partir de la vigencia de la presente Resolución, deberán crear un correo electrónico para uso exclusivo de validación telemática por video pregrabado de usuario; el cual deberá estar publicado en el formulario de registro de cada Institución integrada.

SÉPTIMA. - Las Instituciones integradas al Sistema de Autenticación Única (SAU), en el término de sesenta (60) días, contados a partir de la vigencia de la presente Resolución, deberán permitir a la Entidad Administradora consultar sus bases de datos o repositorio de usuarios, a fin de que se pueda realizar la validación a través de credenciales de instituciones públicas.

DISPOSICIÓN DEROGATORIA

Deróguese la Resolución No. 010-NG-DINARDAP-2020, expedida el 01 de junio de 2020 y la Resolución Nro. 016NG-DINARDAP-2020, emitida el 23 de noviembre de 2020.

La presente Resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dada en el Distrito Metropolitano de Quito, a los 14 de julio de 2022.



Firmado electrónicamente por:

ANGIE KARINA

JIJON

MANCHENO

ANGIE KARINA JIJÓN MANCHENO

DIRECTORA NACIONAL DE REGISTROS PÚBLICOS