



Superintendencia de Notariado y Registro



MANUAL DE GESTIÓN DE USUARIOS Y CONTRASEÑAS

Gestión de Tecnologías de la Información

**SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO**

Código: GTI - MN - 006	Versión: 1	Fecha: 3/Oct/2025
-------------------------------	-------------------	--------------------------

JOSÉ RICARDO ACEVEDO SOLARTE
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS VALENZUELA BUITRAGO
PROFESIONAL OFICINA DE TECNOLOGIA DE LA
INFORMACIÓN
SANTIAGO CAMPO VICTORIA
JEFE OFICINA ASESORA DE PLANEACIÓN

SEPTIEMBRE/2025



República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro



TABLA DE CONTENIDO

INTRODUCCIÓN	4
OBJETIVO	5
ALCANCE	5
GLOSARIO	6
MARCO LEGAL	8
ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS	8
1. ROLES Y RESPONSABILIDADES EN LA ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS	8
2. LINEAMIENTOS GENERALES DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS.....	9
3. GESTIÓN DE USUARIOS	10
4. GESTIÓN DE USUARIOS CLIENTE	15
5. GESTIÓN DE USUARIOS DE PRUEBA.....	17
6. GESTIÓN DE USUARIOS DE SERVICIO	18
7. GESTIÓN DE USUARIOS INVITADOS	19
8. GESTIÓN DE USUARIOS PRIVILEGIADOS O ADMINISTRADORES	20
9. GESTIÓN DE USUARIOS DE AUDITORÍA.....	23
10. MODIFICACIÓN DE USUARIOS.....	23
11. INACTIVACIÓN DE USUARIOS.....	24
12. GESTIÓN DE USUARIOS EN SERVICIOS O APLICATIVOS DE TERCEROS.....	24
DOCUMENTOS ASOCIADOS	25
BIBLIOGRAFÍA	25



**Superintendencia de
Notariado y Registro**



TABLA DE FIGURAS..... 25
TABLA DE TABLAS 25

INTRODUCCIÓN

Superintendencia de Notariado y Registro
Calle 26 No. 13 - 49 Int. 201
PBX 57 + (601) 514 0313
Bogotá D.C., - Colombia
<http://www.supernotariado.gov.co>
correspondencia@supernotariado.gov.co



Superintendencia de Notariado y Registro

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI), la Superintendencia ha desarrollado este Manual de Gestión de Usuarios y Contraseñas el cual establece los lineamientos necesarios para gestionar adecuadamente los accesos y las credenciales en los sistemas de información, garantizando que solo los usuarios autorizados puedan acceder a la información que requieren para el desempeño de sus funciones. El objetivo es minimizar los riesgos asociados la fuga de información y modificaciones no autorizadas. Asegurando la protección de la confidencialidad, integridad y disponibilidad de los activos de información. La implementación de estos controles es esencial para mantener un entorno seguro y confiable, permitiendo que la Superintendencia cumpla con sus responsabilidades de manera eficiente y segura.

Este manual asegura que todos los procesos relacionados con la gestión de usuarios y contraseñas sean evaluados rigurosamente, implementados de manera formal y documentados adecuadamente. Además, define roles y responsabilidades claras para todas las partes involucradas en el proceso de gestión de accesos, desde la creación de cuentas de usuario hasta el control y revisión de los privilegios de acceso y la gestión de contraseñas. Un énfasis especial se centra en la gestión adecuada de los usuarios privilegiados o administradores, quienes tienen acceso ampliado a los sistemas de información y, por lo tanto, representan un mayor riesgo en caso de una mala gestión. Este manual establece directrices específicas para la gestión de estas cuentas, incluyendo la segregación de funciones, la implementación de controles adicionales para el acceso y la revisión periódica de los privilegios asignados, reforzando así la seguridad del entorno de información de la Superintendencia

OBJETIVO

Definir los lineamientos para la creación, modificación y eliminación de usuarios y contraseñas en los sistemas de información de la Superintendencia de Notariado y Registro. Este manual se encuentra articulado con el **PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS**.

ALCANCE

Los lineamientos establecidos en este manual aplican para todos los funcionarios, contratistas y terceros que tienen acceso a la infraestructura tecnológica productiva de la Superintendencia de Notariado y Registro.

Los lineamientos contenidos en este Manual y en el Procedimiento de Administración de Usuarios y Contraseñas deben ser aplicados a partir de la adopción de los documentos en el Sistema Integrado de



Superintendencia de Notariado y Registro

Calidad de la SNR. Así mismo, los Gestores de Aplicaciones propenderán por la implementación de los mismos en los usuarios y contraseñas previamente creados en los diferentes sistemas y aplicativos de la Entidad, en la medida en que sea técnica y/o operativamente posible.

GLOSARIO

- **Acceso:** Permiso otorgado a un usuario para utilizar recursos y sistemas específicos dentro de una organización.
- **Autenticación:** Proceso de verificar la identidad de un usuario antes de permitirle acceder a sistemas o recursos.
- **Autorización:** Proceso de conceder o denegar permisos a los usuarios para acceder a recursos específicos después de haber sido autenticados.
- **Contraseña:** Secuencia de caracteres utilizada para verificar la identidad de un usuario durante el proceso de autenticación.
- **Creación de Usuarios:** Proceso de generar nuevas cuentas de usuario con permisos y accesos específicos según las necesidades del rol asignado.
- **Cuentas de Usuario:** Identificaciones individuales que permiten a los usuarios acceder a sistemas y servicios específicos.
- **Cuentas Privilegiadas:** Cuentas de usuario que tienen permisos adicionales o elevados para realizar tareas administrativas críticas, como configuraciones de sistema y gestión de cuentas.
- **Gestión de Accesos:** Conjunto de políticas y procedimientos utilizados para controlar el acceso de los usuarios a sistemas y datos.
- **Gestión de Contraseñas:** Proceso de creación, almacenamiento, y mantenimiento de contraseñas seguras para proteger el acceso a sistemas y datos.
- **Gestión de Identidades:** Proceso de administrar la identidad y los derechos de acceso de los usuarios dentro de una organización.



Superintendencia de Notariado y Registro

- **Inactivación de Usuarios:** Proceso de desactivar o borrar cuentas de usuario que ya no son necesarias, asegurando que los accesos y permisos asociados sean revocados.
- **Modificación de Usuarios:** Proceso de actualizar la información y permisos de una cuenta de usuario existente para reflejar cambios en el rol o responsabilidades del usuario, una inactivación temporal por periodos de vacaciones o incapacidades se considerará una modificación.
- **OTP (One Time Password):** Es un mecanismo de autenticación que genera una contraseña temporal que solo puede ser usada una vez y tiene una validez limitada en el tiempo.
- **PAM:** Privileged Access Management (PAM), o Gestión de Acceso Privilegiado en español, se refiere a un conjunto de prácticas, políticas y soluciones tecnológicas diseñadas para gestionar y proteger el acceso a cuentas y sistemas con privilegios elevados.
- **Privilegios:** Permisos especiales otorgados a ciertos usuarios que les permiten realizar acciones adicionales o acceder a recursos sensibles.
- **Usuario:** Persona que tiene acceso autorizado a sistemas y recursos de una organización.
- **Usuario Cliente:** Cuentas de usuario asignadas a clientes de la Superintendencia como usuarios de notarías, curadurías, gestores catastrales o entes que cuenten con convenios con la Superintendencia entre otros.
- **Usuario Estándar:** Usuario que tiene acceso básico a los sistemas y recursos necesarios para realizar sus tareas diarias, sin permisos especiales o avanzados (funcionarios, contratistas y pasantes).
- **Usuario de Prueba:** Cuenta de usuario creada temporalmente dentro de un sistema con el propósito de realizar pruebas y validaciones de funcionalidades, configuraciones o actualizaciones antes de su implementación en el entorno de producción.
- **Usuario de Servicio:** Son cuentas genéricas destinadas para la ejecución de tareas de aplicaciones o procesos automáticos en los diferentes componentes de TI.
- **Usuario Privilegiado:** Usuario que tiene permisos avanzados y puede realizar tareas críticas, como configuraciones de sistema y gestión de cuentas, comúnmente denominados como administradores.



Superintendencia de Notariado y Registro

Para efectos del presente manual serán usuarios privilegiados los usuarios Administradores y de Servicio.

- **Usuario no Privilegiado:** Usuarios estándar, Usuarios cliente, Usuarios de auditoría y Usuarios Invitados (Estándar).
- **Usuarios de Auditoría:** Usuarios que tienen privilegios y/o permisos de solo lectura, que tienen fines de revisión o verificación de acciones específicas.

MARCO LEGAL

- Decreto 338 de 2022 “Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”.
- Decreto 767 del 2022 - “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Resolución 500 del 10 marzo de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.

ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS

1. ROLES Y RESPONSABILIDADES EN LA ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS

Los roles que participan para llevar a cabo una adecuada administración de usuarios y contraseñas son los siguientes:

- Registradores, directores, jefes y Coordinadores de área
- Gestor de Infraestructura de Seguridad: Delegado responsable de liderar la formulación, ejecución y seguimiento de la Política de Seguridad de la Información en la Superintendencia de Notariado y Registro.
- Gestores de Aplicaciones: Funcionarios y/o contratistas de la Oficina de Tecnologías de la Información encargados de crear, modificar o eliminar los usuarios.



Superintendencia de Notariado y Registro

- Gestores de Soporte. Colaboradores de la Oficina de Tecnologías de la Información (o del tercero a cargo del soporte de mesa de ayuda) que reciben y gestionan las solicitudes de la mesa de ayuda integral.

Las responsabilidades se encuentran descritas en el desarrollo de este manual y el **PROCEDIMIENTO DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS**.

2. LINEAMIENTOS GENERALES DE ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS

Se definen los siguientes lineamientos generales, que buscan orientar una adecuada administración de usuarios y contraseñas en la Superintendencia de Notariado y Registro:

- Los usuarios sólo deben tener acceso a los servicios que son necesarios para realizar su trabajo, es decir, que las configuraciones deberán garantizar el menor privilegio posible.
- Únicamente los registradores, los directores, jefes o coordinadores de área pueden solicitar la creación o modificación de usuarios.
- La baja o inactivación de usuarios puede ser solicitada por la Oficina de Talento Humano y la Oficina de Contratos, con los soportes de resolución o terminación de contrato correspondientes.
- Todo usuario que esté autorizado (funcionarios y contratistas) para conectarse a alguno de los sistemas de información de la Superintendencia debe accederlos a través de un usuario y una contraseña asignada por la Oficina de Tecnologías de la Información con los roles mínimos requeridos.
- Los sistemas de información cuentan con diversos mecanismos de autenticación, tales como sistemas biométricos, tokens, software OTP, usuarios y contraseñas, entre otros, con el fin de prevenir el acceso no autorizado a los mismos.
- Todos los usuarios (salvo excepciones como usuarios de prueba o usuarios de servicio) deberán manejar segundo factor de autenticación como parámetro de seguridad obligatorio.
- El usuario y la contraseña son únicos e intransferibles, no deben prestarse, no se deben dejar en lugares visibles, todos los registros que se hagan en el sistema bajo dicho usuario son de responsabilidad del propietario de dicha contraseña.



Superintendencia de Notariado y Registro

- Solo se hace entrega de usuarios y contraseñas cuando se encuentre debidamente solicitado y autorizado mediante la herramienta de mesa de ayuda.
- Los servidores, dispositivos de red, recursos informáticos y equipos finales de usuarios deben estar autenticados e identificados en la red con el fin de lograr llevar control de estos.
- La identificación y autenticación para equipos propiedad de la Superintendencia (equipos de cómputo y servidores), debe ser únicamente a través del usuario de directorio activo.
- Los mecanismos de autenticación deben establecer periodos de vigencia y/o renovación, los cuales deben cumplir con las políticas definidas.
- La entidad administra usuarios de los sistemas de información principales a través de una solución centralizada de gestión de identidades, existen sistemas legados que no permiten esta integración por lo cual serán actualizados y posteriormente enlazados a este gestor.
- Los mecanismos de autenticación permitirán la trazabilidad de los accesos concedidos a los usuarios y las actividades realizadas (Adiciones, eliminaciones, modificaciones etc...) en cada uno de los recursos informáticos.

3. GESTIÓN DE USUARIOS

Únicamente los usuarios y contratistas de la Superintendencia tendrán derecho a solicitar (a través de sus jefes) un usuario para acceder a las aplicaciones y servicios de la entidad.

Para que los usuarios puedan ser creados, se tiene que realizar una solicitud de creación de usuario a través de la mesa de ayuda, remitiendo como mínimo la siguiente documentación:



FUNCIONARIO	CONTRATISTA	PASANTES Y/O JUDICANTES	USUARIOS POR CONVENIOS / CONTRATOS
<ul style="list-style-type: none"> • Formato de administración de usuarios. • Resolución o Acta de posesión. 	<ul style="list-style-type: none"> • Copia del contrato • Copia del acta de inicio firmada. • Copia del acta de designación de supervisión. • Formato de Administración de Usuarios. 	<ul style="list-style-type: none"> • Formato de administración de usuarios. • Resolución. • Acta de posesión. 	<ul style="list-style-type: none"> • Copia del contrato, convenio o acuerdo de servicio que justifica la creación del usuario. • Formato de administración de usuarios.

Tabla 1 Documentación Requerida para la solicitud de creación de usuarios

Dependiendo de los sistemas de información solicitados, podrán existir requerimientos particulares que podrán analizarse de manera particular según el convenio, sistema de información o el tipo de rol a solicitar.

3.1 GESTOR DE IDENTIDADES (IGA)

La entidad cuenta con un sistema de gestión de identidades, que busca facilitar la centralización de las actividades de administración de usuarios, es decir, creación, modificación e inactivación de usuarios dentro de los sistemas de información de la Superintendencia, incluyendo el directorio activo y sistemas como SIR, VUR, SIDT entre otros, por lo tanto, las políticas que se aplican para directorio activo a nivel de usuarios y contraseñas serán acogidas y aplicadas por el sistema de gestión de identidades dado su integración con el directorio activo de la entidad.

3.2 USUARIOS ESTÁNDAR EN DIRECTORIO ACTIVO, GESTOR DE IDENTIDADES Y NUEVOS SISTEMAS DE INFORMACIÓN

La composición del nombre de usuario estará determinada por la aplicación en la cual se realizará la creación, sin embargo, las aplicaciones estarán conectadas al directorio o al gestor de identidades, cumpliendo la siguiente composición:

El nombre de usuario estándar para los servicios se define siguiendo las siguientes reglas:



Superintendencia de Notariado y Registro

1. El primer nombre, seguido del signo punto (.) y a continuación el primer apellido en minúscula.

Ejemplo:

- Nombre: Ana Carolina García Díaz
- **Usuario de Dominio:** ana.garcia

2. De encontrarse un usuario existente con las mismas características deberá añadirse la primera letra del segundo nombre para realizar la diferenciación.

Ejemplo:

- Nombre: Ana Milena García Rodríguez
- **Usuario de Dominio:** anam.garcia

3. De encontrarse un usuario existente con las 2 reglas anteriores, el usuario se deberá crear empleando la primera letra del **SEGUNDO** apellido, seguido del primer apellido en minúscula y usando la primera letra del segundo apellido.

Ejemplo:

- Nombre: Ana Maria Garcia Vasquez
- **Usuario de Dominio:** anam.garciav

En casos excepcionales, donde la conformación del usuario pueda presentar una interpretación inadecuada o representativa a palabras no apropiadas el usuario podrá solicitar mediante mesa de ayuda, el cambio de composición de su usuario en un periodo no máximo a 3 días hábiles posterior a la entrega del usuario inicial.

NOTA: La creación de los nombres de usuario con el estándar primernombre.primerapellido se llevará a cabo a partir de la liberación de este manual. Sin embargo, en los sistemas SIR, VUR y SIDT realizarán la homologación de nombres de usuario antiguos a este nuevo estándar y tendrán hasta 4 meses después de la liberación para ejecutar esta actividad.

3.3 USUARIOS EN CORREO ELECTRÓNICO

Para la designación de correo electrónico, se utilizará el nombre de usuario de dominio indicado previamente, todo sucedido del dominio@supernotariado.gov.co.



Superintendencia de Notariado y Registro

Ejemplo:

- Si el nombre de usuario es ana.garcia el correo electrónico será: ana.garcia@supernotariado.gov.co

Tanto el usuario de dominio o de correo electrónico, son los mismos que se emplean para ingresar a todos los servicios de productividad y colaboración disponibles en la nube de la Superintendencia, el usuario de dominio también aplica para el acceso de la mayoría de los sistemas de información de la entidad salvo excepciones indicadas en este manual.

NOTA: Podrán solicitarse usuarios genéricos de correo electrónico, **garantizando que exista un único responsable para su adecuado uso y administración**, también las solicitudes estarán sujetas a disponibilidad de recursos y licenciamiento.

3.4 USUARIOS APLICATIVO FOLIO

Es un sistema legado, la creación de usuarios puede tener hasta ocho caracteres alfanuméricos. Los usuarios se crean con base al rol y un consecutivo numérico.

3.5 USUARIOS APLICATIVO SIN

Es un sistema legado, a partir de la liberación de este manual, se acogerá a las directrices de creación de usuarios estándar.

3.6 USUARIOS APLICATIVO IRIS

Es un sistema legado, a partir de la liberación de este manual, se acogerá a las directrices de creación de usuarios estándar.

3.7 USUARIOS APLICATIVO HGFI (Herramienta de Gestión Financiera Integral)

A partir de la liberación de este manual, se acogerá a las directrices de creación de usuarios estándar.

3.8 MANEJO DE CONTRASEÑAS PARA USUARIOS ESTÁNDAR

Las contraseñas en los sistemas de información cumplen con las siguientes características de manejo:



Superintendencia de
Notariado y Registro

Característica	Descripción	DOMINIO, IGA, SISG, SIR, CORREO, VUR
Composición	Tipo de caracteres exigidos mínimos que se deben incluir en el contenido de la contraseña.	La contraseña deberá crearse con Mayúsculas, minúsculas, numéricos y especiales. Ej. AAAaaa123@\$%#. Excepción: Folio y SIN, es opcional esta característica
Longitud mínima	Número mínimo de caracteres que puede contener la contraseña de un usuario.	Al menos 8 caracteres
Cambio mandatorio de contraseña	Tiempo o periodo máximo indicado para realizar el cambio periódico de la contraseña. Excepción: Verificar Folio	Cada 3 meses Excepción: SIN nunca expira la contraseña.
Notificación de Vencimiento de contraseña	Tiempo en el que el sistema debe informar con anticipación a cada uno de los usuarios el vencimiento de la contraseña.	Al menos 10 días antes del vencimiento. Excepción: Folio, ASEC, SIN no soporta.
Historia	Opción de que el sistema recuerde un número determinado de contraseñas anteriores, y evite que sean utilizadas nuevamente por el usuario.	Últimas 2 contraseñas Excepción: Iris (No soporta) Folio (1 contraseña) SIN (No soporta) ASEC (No soporta)
Contraseñas iniciales o reestablecidas	Forzar al usuario a cambiar la contraseña antes que se complete el siguiente proceso de inicio de sesión, cuando son emitidas por primera vez o reestablecidas por un administrador. Excepción: Folio, Iris	Forzar al usuario a cambiar la contraseña antes que se complete el siguiente proceso de inicio de sesión, cuando son emitidas por primera vez o reestablecidas por un administrador. SIN (No soporta)

Tabla 2 Características de manejo de contraseñas



Superintendencia de Notariado y Registro

NOTA: Los sistemas legados de la entidad, no cuentan con la opción de garantizar las características de contraseñas anteriormente descritas. Una vez sean migrados a nuevos sistemas, se garantizará que dichos sistemas si cumplan con estas características. Adicionalmente, todos los nuevos sistemas de información que se aprovisionen posterior a la liberación de este manual cumplirán con lo descrito en estos requisitos.

4. GESTIÓN DE USUARIOS CLIENTE

Los usuarios cliente son usuarios externos de consulta o de solicitud de trámites de la Superintendencia, como usuarios de notarias, curadurías, entes que cuenten con convenios o acuerdos de servicio con la Superintendencia o la ciudadanía en general.

Los lineamientos para la administración de usuarios tipo cliente que gestiona la Superintendencia son los siguientes:

- Para los sistemas de información de cara a la ciudadanía, los usuarios podrán registrarse y consumir los servicios que ofrece la Superintendencia según sea el caso.
- Para usuarios cliente que requieran privilegios específicos, como usuarios de convenios, acuerdos de servicio y demás, será la Superintendencia la que gestione la creación y aprobación de los permisos como usuarios estándar o privilegiados según sea el caso y bajo las consideraciones que la entidad disponga, sin embargo, dentro de la creación del usuario **deberá tenerse en cuenta algún identificador que permita deducir que entidad o empresa tiene bajo su custodia el usuario más el nombre del responsable de dicho acceso.**
- Aplicativos como REL, VUR y SISG generan usuarios CLIENTE por cuenta de notarias, curadurías y consulados, convenios y acuerdos de servicio, aunque a su vez también funcionan para usuarios internos de la entidad.

NOTA: Se establece que, para las solicitudes de creación, modificación y/o inactivación de usuarios CLIENTE en la aplicación VUR se deberá emplear el **FORMATO CREACIÓN DE USUARIOS VENTANILLA ÚNICA DE REGISTRO – VUR.**

- A través de la integración con carpeta ciudadana se gestionan accesos de consulta para la ciudadanía, los usuarios son creados en el autenticador de la agencia nacional digital y no son controlados por la Superintendencia.



Superintendencia de Notariado y Registro

- Se generan accesos a través de la plataforma X-ROAD (plataforma de interoperabilidad) las cuales también manejan con usuarios gestionados por convenios y acuerdos de servicio con otras entidades. Los usuarios de los servicios son gestionados como usuarios estándar como se indica en la documentación técnica vigente de los servicios de interoperabilidad.

4.1 USUARIOS CLIENTE EN APLICACIONES DE LA SUPERINTENDENCIA

Los usuarios cliente en las aplicaciones de la Superintendencia se aprovisionan con la siguiente estructura:

TIPO DE DOCUMENTO (CC, TI, NIT, CE) + NÚMERO DE DOCUMENTO DE IDENTIFICACIÓN

- Ejemplo 1: Si un ciudadano tiene cédula de ciudadanía 12.345.678, el usuario sería **CC12345678**
- Ejemplo 2: Si un ciudadano tiene cédula de extranjería 98.765.432, el usuario sería **CE98765432**

NOTA: El aprovisionamiento de los usuarios con esta estructura se realizará a partir de la liberación del manual.

4.2 MANEJO DE CONTRASEÑAS PARA USUARIOS CLIENTE

Para las contraseñas de los usuarios cliente se cumplen con las siguientes características de manejo:

Característica	Descripción	Configuración
Composición	Tipo de caracteres exigidos mínimos que se deben incluir en el contenido de la contraseña.	La contraseña deberá crearse con Mayúsculas, minúsculas, numéricos y especiales. Ej. AAAaaa123@\$\$%#.
Longitud mínima	Número mínimo de caracteres que puede contener la contraseña de un usuario.	Al menos 8 caracteres
Historia	Opción de que el sistema recuerde un número determinado de contraseñas anteriores, y evite que sean utilizadas nuevamente por el usuario.	Deberá recordar por lo menos las últimas 2 contraseñas Excepción - REL

Tabla 3 Características de manejo de contraseñas para Usuarios Cliente



Superintendencia de Notariado y Registro

Los usuarios podrán registrarse con cuentas de correo Hotmail y Gmail, sin embargo, estas no podrán ser el login de los usuarios, deberá ser su número de identificación o el usuario otorgado por la Superintendencia.

5. GESTIÓN DE USUARIOS DE PRUEBA

Los usuarios de prueba son necesidades eventuales para el despliegue de servicios o para la ejecución de pruebas para mejoras en los sistemas. Es responsabilidad del Administrador de la plataforma la creación y control de estos usuarios, todo usuario de prueba deberá solicitarse mediante un requerimiento a través de la mesa de ayuda integral o por correo electrónico al administrador para su revisión.

5.1 USUARIOS DE PRUEBA EN SISTEMAS DE INFORMACIÓN:

Los usuarios de prueba deberán estructurarse de la siguiente manera:

- prueba.plataforma.proveedor/primer letra nombre + apellido usuario solicitante.
- Ej. prueba.sara.jvalenzuela
- Ej. prueba.sara.evolution

La cuenta deberá entregarse al líder de proyecto o al solicitante del usuario de prueba quien se hará responsable de cualquier acción durante su funcionamiento.

Los usuarios de prueba podrán ser solicitados por el registrador, director, jefe de área, coordinador o por el Oficial de Seguridad, indicando la temporalidad del usuario, la cual no deberá superar 1 mes, después de este mes deberá generarse un nuevo requerimiento, el administrador que otorgue estos usuarios deberá llevar un control estricto de los mismos.

Una vez finalizadas las pruebas en los sistemas, estos usuarios deben ser inactivados de manera inmediata para mantener la seguridad del entorno.

5.2 MANEJO DE CONTRASEÑAS PARA USUARIOS DE PRUEBA

Para las contraseñas de los usuarios de prueba se cumplen con las siguientes características de manejo:



Característica	Descripción	Configuración
Composición	Tipo de caracteres exigidos mínimos que se deben incluir en el contenido de la contraseña.	La contraseña deberá crearse con Mayúsculas, minúsculas, numéricos y especiales. Ej. AAAaaa123@%\$#.
Longitud mínima	Número mínimo de caracteres que puede contener la contraseña de un usuario.	Al menos 8 caracteres
Historia	Opción de que el sistema recuerde un número determinado de contraseñas anteriores, y evite que sean utilizadas nuevamente por el usuario.	Deberá recordar por lo menos la última contraseña

Tabla 4 Características de manejo de contraseñas para Usuarios de Prueba

6. GESTIÓN DE USUARIOS DE SERVICIO

Al ser usuarios que se emplean para la ejecución de tareas de aplicaciones o procesos automáticos en los diferentes componentes de TI, estos únicamente pueden ser solicitados **exclusivamente por el personal de la Oficina de Tecnologías de la Información.**

La solicitud de estos usuarios podrá ser realizada a través de la mesa de ayuda diligenciando el formato correspondiente, solicitando los roles y privilegios exclusivamente necesarios para el funcionamiento de las aplicaciones. Dicha solicitud deberá ser validada por el Administrador de la plataforma correspondiente.

Las cuentas de servicio únicamente podrán ser empleadas o administradas por el personal de la Superintendencia y serán responsabilidad del solicitante de su creación, debe existir constancia de la creación del usuario y de quien lo gestionará.

El administrador de cada aplicación y/o plataforma debe mantener actualizados los registros de usuarios de servicio a través del **FORMATO – MATRIZ DE REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO.**



6.1 MANEJO DE CONTRASEÑAS PARA USUARIOS DE SERVICIO

Característica	Descripción	Configuración
Composición	Tipo de caracteres exigidos mínimos que se deben incluir en el contenido de la contraseña.	La contraseña deberá crearse con Mayúsculas, minúsculas, numéricos y especiales. Ej. AAAaaa123@\$%#.
Longitud mínima	Número mínimo de caracteres que puede contener la contraseña de un usuario.	Al menos 16 caracteres

Tabla 5 Características de manejo de contraseñas para Usuarios de Servicio

7. GESTIÓN DE USUARIOS INVITADOS

Los usuarios invitados son usuarios que se pueden generar para proveedores u otros usuarios temporales, para simular el comportamiento de un usuario normal dentro de una aplicación o brindar soporte de esta, pueden tener características de usuarios privilegiados o no privilegiados según corresponda. Teniendo en cuenta el tipo de usuario solicitado, se debe seguir con el procedimiento correspondiente. La diferencia radicará en la temporalidad de este usuario, la cual deberá estar controlada y documentada.

Durante periodos de despliegue e implementación de nuevas soluciones los proveedores al ser los responsables del sistema y su estabilización, podrán contar con usuarios por el tiempo que dure dicha implementación.

7.1 GESTIÓN DE USUARIOS INVITADOS

Los usuarios invitados podrán ser solicitados por el Registrador, director, jefe de Área y/o Coordinador, adjuntando la documentación indicada en la sección 6.3 de este manual, indicando la temporalidad del usuario, la cual no deberá superar 1 mes, después de este mes deberá generarse un nuevo requerimiento.

Nota: Deberá exigirse acuerdo de confidencialidad para aquellos que no tengan una relación contractual vigente con la Superintendencia.



7.2 MANEJO DE CONTRASEÑAS PARA USUARIOS INVITADOS

Según el tipo de usuario invitado solicitado, se deberán aplicar las políticas de contraseñas correspondientes, sea privilegiado o no privilegiado.

8. GESTIÓN DE USUARIOS PRIVILEGIADOS O ADMINISTRADORES

Para la creación, modificación o baja de accesos privilegiados a los sistemas de información que gestiona la Oficina de Tecnologías de la Información se deben tener en cuenta los siguientes lineamientos:

- Todos los usuarios privilegiados deben ser usuarios identificables, no podrán ser usuarios genéricos salvo excepciones específicas delimitadas en este manual.
- Los administradores de las aplicaciones o líderes técnicos darán visto bueno a las solicitudes de creación de usuarios privilegiados y las aprobaciones finales serán brindadas por cada coordinador según corresponda.
- La mesa de ayuda validará el **FORMATO DE ADMINISTRACIÓN DE USUARIOS** debidamente diligenciado y firmado.
- La estructura para la creación de usuarios privilegiados será la siguiente:
 - Si es un usuario de la Superintendencia, deberá aplicarse la misma estructura de nombre establecida para los usuarios estándar, es decir:
 - primernombre.primerapellido.
 - Si es un usuario de un proveedor, deberá aplicarse la siguiente estructura:
 - empresa.primernombre.primerapellido.
 - Si existen coincidencias en usuarios deben aplicarse las reglas establecidas para creación de usuarios estándar establecidas en la sección 6.3.2.
- El administrador de cada aplicación y/o plataforma debe mantener actualizados los registros de usuarios privilegiados con las respectivas evidencias. Cada vez que se ejecute un requerimiento que involucre la creación o modificación de accesos privilegiados, estos registros se deben actualizar. Finalmente, todo acceso privilegiado deberá estar respaldado por el requerimiento que soporte los privilegios otorgados.
- Las matrices de usuarios privilegiados deberán construirse empleando el **FORMATO – MATRIZ DE REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO**, llevando registro histórico de las creaciones, modificaciones y/o eliminaciones de los usuarios.



Superintendencia de Notariado y Registro

- El Oficial de Seguridad de la Información podrá requerir en cualquier momento a los administradores el **FORMATO – MATRIZ DE REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO**, para efectos de auditoría.
- Las cuentas privilegiadas nativas como (root, admin, sa etc...) deberán estar debidamente asignadas, teniendo un único responsable quien asumirá todas las acciones que se ejecuten a través de estas. La asignación de las cuentas privilegiadas nativas deberá estar debidamente documentado por parte del administrador de cada plataforma.
- Los usuarios privilegiados en plataformas Windows estarán controlados por la herramienta PAM y dichos privilegios serán otorgados a través de los grupos en directorio activo y por parte del Administrador de esta solución de seguridad, de igual forma la herramienta PAM registrará los logs de eventos de cada usuario privilegiado.
- La eliminación de accesos privilegiados no requiere de aprobaciones, sin embargo, si deberán escalarse requerimientos para la inactivación de usuarios como si fuese cualquier tipo de usuario. Los responsables de la eliminación deben asegurarse de actualizar los registros en **FORMATO – MATRIZ DE REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO** inmediatamente después de la baja.
- Únicamente el jefe de la Oficina de Tecnologías de la Información podrá solicitar de forma directa la asignación de accesos privilegiados para usuarios, siempre y cuando tengan relación contractual o laboral con la Superintendencia, esta autorización deberá estar por escrito.

8.1 GESTIÓN DE USUARIOS PRIVILEGIADOS EN PERIODOS DE REEMPLAZOS, VACACIONES O EVENTUALIDADES.

Si el funcionario, contratista o tercero de la Superintendencia por algún motivo sale a periodo de vacaciones, incapacidad o cualquier situación atípica que requiera entregar las credenciales para que la operación pueda continuar, debe notificarse inmediatamente al personal la Superintendencia sobre esta situación, teniendo en cuenta lo siguiente:

- Se debe reportar al nuevo responsable y el tiempo estimado de la asignación temporal para tener la trazabilidad de la responsabilidad de uso frente a los usuarios privilegiados.
- No se realizarán modificaciones a los privilegios del usuario que estará ausente, se realizará una inactivación temporal de la cuenta, con el objetivo de impactar en la menor medida posible el retorno del usuario después de su periodo de ausencia.
- Se debe realizar el respectivo procedimiento de creación o modificación de accesos según sea el



caso, para el reemplazante de la persona en periodo de vacaciones, incapacidad o situación atípica.

8.2 MANEJO DE CONTRASEÑAS PARA USUARIOS PRIVILEGIADOS

Todas las cuentas de administración deberán cumplir con las siguientes características de manejo de las contraseñas:

Característica	Descripción	CONDICIÓN
Composición	Tipo de caracteres exigidos mínimos que se deben incluir en el contenido de la contraseña. Excepción: Folio	Contraseña: Mayúsculas, minúsculas, numéricos y especiales. Ej. AAAaaa123@\$%#.
Longitud mínima	Número mínimo de caracteres que puede contener la contraseña de un usuario.	Al menos 12 caracteres
Notificación de Vencimiento de contraseña	Tiempo en el que el sistema debe informar con anticipación a cada uno de los usuarios el vencimiento de la contraseña. Excepción: Verificar Folio	Al menos 10 días antes del vencimiento.
Historia	Opción de que el sistema recuerde un número determinado de contraseñas anteriores, y evite que sean utilizadas nuevamente por el usuario.	Últimas 2 contraseñas
Cambio mandatorio de contraseña	Tiempo o periodo máximo indicado para realizar el cambio periódico de la contraseña. Excepción: Verificar Folio	Cada 4 meses

Tabla 6 Características de manejo de contraseñas para Usuarios Privilegiados



9. GESTIÓN DE USUARIOS DE AUDITORÍA

Los usuarios de auditoría se crean con el propósito de monitorear actividades en los sistemas de información, garantizando la integridad, seguridad, y trazabilidad en la operación. Estos usuarios no deben tener privilegios de modificación o administración, salvo en situaciones excepcionales debidamente justificadas, a continuación, se indican los lineamientos correspondientes:

- La creación de usuarios de auditoría podrá ser solicitada únicamente por los siguientes roles: Auditores Internos o externos, Oficial de Seguridad, Responsables de cumplimiento o de control interno, en el contexto de evaluaciones de conformidad o auditorías internas.
- Toda solicitud de creación de un usuario de auditoría debe estar respaldada por un requerimiento formal, en el que se detallen los motivos, el alcance, y el periodo de vigencia de los accesos solicitados.
- Los usuarios de auditoría tendrán permisos de solo lectura en los sistemas que se auditen, excepto en casos donde se requiera ejecutar consultas o revisiones específicas, lo cual deberá estar claramente documentado y autorizado. Así mismo, el acceso debe estar limitado a los recursos estrictamente necesarios para la auditoría solicitada.

10. MODIFICACIÓN DE USUARIOS

Para la modificación de permisos de usuario, se solicitará la documentación indicada en la sección 6.3 del manual para solicitudes relacionadas con Cambios de Rol/Cargo o Cambios de Área. En particular se considerarán modificaciones las siguientes situaciones:

- **Cambio de rol/cargo:** Esta modificación indica que el funcionario permanece en la misma área, pero tendrá un cambio en el rol o cargo que desempeña en esta y requiere cambios en sus permisos o privilegios en los sistemas de información. El área que requiere el cambio de rol del funcionario debe diligenciar el Formato de Administración de Usuarios y los demás documentos indicados en la sección 6.3 del manual.
- **Cambio de área:** Esta modificación indica que el funcionario permanece en la misma área, pero tendrá un cambio en el rol o cargo que desempeña en esta y requiere cambios en sus permisos o privilegios en los sistemas de información. El área que requiere el cambio de rol del funcionario debe diligenciar el Formato de Administración de Usuarios y los demás documentos indicados en la sección 6.3 del manual.



Superintendencia de Notariado y Registro

- **Salidas por Vacaciones:** La dirección de talento humano, deberá informar a la oficina de tecnologías de la información vía correo electrónico las salidas a vacaciones del personal, indicando la fecha de salida y la fecha de reincorporación, para realizar las gestiones en los sistemas de información de manera oportuna y evitar así posibles incidentes durante la ausencia de los funcionarios.

Nota: Solo bajo situaciones excepcionales, los registradores, directores o jefes de área podrán solicitar que la cuenta de un funcionario pueda reactivarse por cuestiones críticas de servicio de la entidad y tomarán responsabilidad sobre las acciones efectuadas con estas cuentas. Dichas solicitudes deberán escalar directamente al Jefe de la Oficina de Tecnologías de la Información para su revisión.

11. INACTIVACIÓN DE USUARIOS

La baja o inactivación de usuarios puede ser solicitada únicamente por la Dirección de Talento Humano y la Dirección de Contratación, con la notificación oficial de terminación o cesión de contrato o vínculo laboral correspondientes, esta notificación debe realizarse vía correo electrónico a la mesa de ayuda y de manera masiva si la situación así lo amerita. La inactivación del usuario, se realizará a partir de la fecha de la terminación o cesión del contrato o vínculo laboral, conforme con el soporte allegado por la Dirección de Talento Humano o de Contratación, respectivamente.

Los Registradores, directores y jefes son los únicos autorizados para solicitar el bloqueo temporal de un usuario de forma directa, bajo situaciones y justificaciones excepcionales que comprometan los intereses de la Superintendencia, esta solicitud solo podrá hacerse de forma directa al jefe de la Oficina de Tecnologías de la Información, quien dará el aval si lo considera pertinente.

Todas las cuentas al ser inactivadas tendrán un periodo de retención de la información por 3 años, sea correo o onedrive, si se realiza la solicitud correspondiente.

12. GESTIÓN DE USUARIOS EN SERVICIOS O APLICATIVOS DE TERCEROS

Se consideran servicios o aplicativos de terceros aquellos sistemas o plataformas administrados y soportados por entidades externas a la Superintendencia de Notariado y Registro, ya sean organismos nacionales o empresas privadas que otorgan acceso a sus aplicaciones.

Con el fin de garantizar un manejo adecuado de las credenciales y la administración de accesos en estos servicios, se establecen los siguientes lineamientos:



Superintendencia de Notariado y Registro

- **Gestión de soporte:** Cualquier solicitud de soporte técnico o asistencia relacionada con aplicaciones de terceros deberá ser escalada directamente a la entidad responsable del servicio.
- **Definición de credenciales y parámetros de seguridad:** La nomenclatura de usuario, políticas de seguridad, requisitos de contraseña y demás configuraciones de autenticación serán determinados por la entidad externa que administra el servicio.
- **Procesos de gestión de usuarios:** Las solicitudes de creación, modificación o eliminación de usuarios en servicios de terceros podrán ser canalizadas a través de la Oficina de Tecnologías de la Información mediante un requerimiento formal a la mesa de ayuda integral (esto es opcional). Estas solicitudes serán remitidas al área de la Superintendencia responsable del contacto con la entidad externa, a fin de gestionar el acceso conforme a los procedimientos establecidos por dicha entidad, o si el solicitante así lo prefiere, podrá contactar directamente al área correspondiente para gestionar estos requerimientos.
- **Custodia de credenciales:** Cada área de la Superintendencia es responsable de la adecuada protección y administración de las credenciales de acceso (usuarios y contraseñas) a los servicios de terceros, asegurando su uso exclusivo para los fines autorizados y evitando su divulgación no autorizada.

DOCUMENTOS ASOCIADOS

No aplica

BIBLIOGRAFÍA

No aplica.

TABLA DE FIGURAS

No aplica.

TABLA DE TABLAS

Tabla 1 Documentación Requerida para la solicitud de creación de usuarios 11



**Superintendencia de
Notariado y Registro**

Tabla 2 Características de manejo de contraseñas 14

Tabla 3 Características de manejo de contraseñas para Usuarios Cliente 16

Tabla 4 Características de manejo de contraseñas para Usuarios de Prueba..... 18

Tabla 5 Características de manejo de contraseñas para Usuarios de Servicio 19

Tabla 6 Características de manejo de contraseñas para Usuarios Privilegiados..... 22

VERSIÓN DE CAMBIOS			
Código:	Versión:	Fecha:	Motivo de la actualización:
	1	3 de Octubre de 2025	Se hace necesario ajustar la documentación en el marco del fortalecimiento institucional con el fin de alinearlos al Sistema Integrado de Gestión y el nuevo modelo por procesos de la Entidad.

ELABORACIÓN Y APROBACIÓN			
ELABORÓ	APROBÓ	REVISIÓN METODOLOGICA	Vo. Bo. Oficina Asesora de Planeación
Juan Carlos Valenzuela Buitrago	José Ricardo Acevedo Solarte	Juan Sebastián Ávila	Santiago Campo Victoria
Oficina de tecnología de la Información y las Comunicaciones	Jefe Oficina de Tecnología de la Información	Contratistas OAP	Jefe Oficina Asesora de Planeación
Fecha: 22 de septiembre 2025	Fecha: 25 de septiembre 2025	Fecha: 30 de septiembre 2025	Fecha de Aprobación: 3 de Octubre 2025