PROCEDIMIENTO: ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS		
OBJETIVO:		Controlar la creación, modificación e inactivación de usuarios en los sistemas de información de la Superintendencia de Notariado y Registro mediante la implementación de controles adecuados durante el ciclo de vida de los usuarios y el uso de contraseñas seguras, para proteger la confidencialidad, integridad y disponibilidad de los servicios tecnológicos de la entidad.
ALCANCE:	**Limite Inicial:**	Gestionar las solicitudes para la creación, modificación e inactivación de usuarios en los sistemas de información de la SNR.
	¿Qué hace?	Gestionar la administración de usuarios y contraseñas.
	Limite Final:	Solicitudes de creación, modificación e inactivación de usuarios ejecutados y documentados, cumpliendo con los principios de mínimo privilegio
PRODUCTOS:		Solicitudes de creación, modificación e inactivación en los sistemas de información gestionadas adecuadamente.
RESPONSABLE:		Estratégico: Jefe de Oficina de Tecnologías de la Información Operativo: Coordinador Grupo de Servicios Tecnológicos

1. 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.

Dirección IP: Número único de identificación de un dispositivo conectado a una red, como Internet, que facilita la comunicación entre PC, teléfonos y otros dispositivos conectados.

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.

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.

Puertos TCP / UDP: Número lógico que permite identificar qué servicio o aplicación de un dispositivo debe recibir los datos que llegan por la red.

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 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 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 no Privilegiado: Usuarios estándar, Usuarios cliente, Usuarios de auditoría y Usuarios Invitados (Estándar).

Usuario Privilegiado: Usuario que tiene permisos avanzados y puede realizar tareas críticas, como configuraciones de sistema y gestión de cuentas, comúnmente denominados como administradores. Para efectos del presente manual serán usuarios privilegiados los usuarios Administradores y de Servicio.

Usuario: Persona que tiene acceso autorizado a sistemas y recursos de una organización.

Usuarios de Auditoría: Usuarios que tienen privilegios y/o permisos de solo lectura, que tienen fines de revisión o verificación de acciones específicas.

VPN Cliente: Permite que un usuario se conecte de forma segura a una red privada desde una ubicación externa, como si estuviera conectado directamente a esa red.

VPN Permanente: Mantiene un túnel seguro disponible de forma constante para que las redes puedan comunicarse entre sí.

VPN Temporal: Conexión segura que se utiliza durante un tiempo limitado para acceder a una red o recurso privado.

2. CONDICIONES GENERALES:

2.1. Normatividad: No aplica.

2.2. Políticas de operación

1. Este procedimiento aplica para Sistemas de Información administrados por la Superintendencia de Notariado y Registro. Para sistemas de terceros (externos) podrá coordinarse directamente con el área de la Superintendencia responsable del contacto con la entidad externa o podrá abrirse un requerimiento en la mesa de ayuda integral si dicho sistema externo ha sido enrolado en los catálogos de servicios de tecnología.

2. Toda solicitud de creación, modificación y eliminación de usuarios deberá estar soportada mediante registro en la plataforma de mesa de ayuda integral.

3. Toda creación y modificación de usuarios privilegiados debe tener una justificación y visto bueno por parte de los líderes de cada pilar de los sistemas de información (Gestor de Infraestructura, Gestor de Bases de Datos, Gestor de Seguridad Informática entre otros), así mismo deberá tener una aprobación por parte del coordinador correspondiente.

4. Las solicitudes de creación y modificación de usuarios deberán ser validadas por parte de los jefes directos quienes tendrán la responsabilidad de una adecuada segregación de roles y responsabilidades en los sistemas de información.

5. Los usuarios no privilegiados para efectos de este procedimiento son: Usuarios estándar, Usuarios cliente, Usuarios de auditoría y Usuarios Invitados (Estándar).

6. Los reportes de salida de vacaciones, licencias o inactivaciones temporales serán tramitados como modificaciones de usuarios, las solicitudes de inactivación de usuarios son bajas definitivas por salida del funcionario o finalizaciones de contrato.

7. Las oficinas de contratación y de talento humano, podrán realizar reportes masivos para inactivación de personal de acuerdo con el flujo de bajas y periodos de vacaciones que puedan darse en determinados periodos del año.

8. La creación y/o asignación de permisos a buzones genéricos se realizará mediante solicitud autorizada a través del respectivo formato, garantizando trazabilidad y control por parte del área de TI.

9. La creación, modificación o eliminación de permiso para acceso a la red mediante VPN cliente para los usuarios de la entidad deberá ser solicitada por el funcionario o contratista de la dependencia y aprobado únicamente por el jefe de la dependencia o coordinadores del área solicitada y posteriormente se da la viabilidad técnica de la solicitud por parte de la coordinación de servicios tecnológico de la OTI a través del respectivo formato, garantizando trazabilidad y control por parte del área de TI.

10. Para la ejecución de este procedimiento, se deben tener en cuenta las demás condiciones y políticas establecidas en el Manual de Administración de Usuarios y Contraseñas.

DESCRIPCIÓN DE ACTIVIDADES DEL PROCEDIMIENTO:

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
INICIO **1. ¿QUÉ TIPO DE USUARIO SE DESEA GESTIONAR?**	**1.1.** ¿Qué tipo de usuario se desea gestionar? Privilegiado o de Servicio: Ir a la actividad No. 2 No Privilegiado: Ir a la actividad No. 11.	Registradores, directores, Jefes y Coordinadores Usuarios Oficina de TI	Correo Electrónico
2. SOLICITAR VISTO BUENO DE LOS ACCESOS PRIVILEGIADOS.	**2.1** Solicitar visto bueno de los accesos privilegiados al líder técnico correspondiente que otorga los permisos, con la justificación correspondiente.	Usuarios Oficina de TI	Correo Electrónico
3. ¿LA SOLICITUD DE ACCESOS PRIVILEGIADOS ES APROPIADA?	**3.1** ¿La solicitud de accesos privilegiados es pertinente? **Si:** Ir a la actividad No. 4. **No**: Ir a la actividad No. 26, indicando la causa de rechazo de la solicitud de privilegios.	Líderes Técnicos de Sistemas de Información	Correo Electrónico
4. SOLICITAR AUTORIZACIÓN AL COORDINADOR CORRESPONDIENTE	**4.1** Solicitar autorización al coordinador correspondiente vía correo electrónico, adjuntando el visto bueno del líder técnico	Usuario Solicitante	Correo Electrónico
5. ¿SE APRUEBA LA SOLICITUD DE ACCESOS PRIVILEGIADOS?	**5.1** ¿Se aprueba la solicitud de accesos privilegiados? **Si:** Ir a la actividad No. 6. **No:** Ir a la actividad No. 26, indicando la causa de rechazo de la solicitud de privilegios.	Coordinadores Oficina de Tecnologías	Correo Electrónico
6. GENERAR REQUERIMIENTO EN LA MESA DE AYUDA	**6.1.** Crear la solicitud en la mesa de ayuda, de acuerdo con el Procedimiento de Mesa de Ayuda Integral, adjuntando el formato diligenciado. Si se trata de accesos privilegiados, incluir los correos de autorización y VoBo de las actividades 3 y 5. **6.2.** En el caso de los buzones de correo institucional genéricos, se debe diligenciar el Formato de creación y/o asignación de permisos a buzones genéricos.	Solicitante de los accesos	Ticket en mesa de ayuda Formato de Administración de Usuarios Diligenciado Soportes de autorización y VoBo (Si aplica) Formato de creación y/o asignación de permisos a buzones genéricos.
7. ¿LA DOCUMENTACIÓN SE ENCUENTRA COMPLETA	**7.1.** ¿La documentación se encuentra completa? **Si:** Ir a la actividad No. 8. **No:** Regresar el ticket al solicitante, indicando la información faltante.	Gestor de Mesa de Ayuda	Ticket de Mesa de Ayuda
8. ASIGNAR EL REQUERIMIENTO A LOS ADMINISTRADORES DE SISTEMAS DE OTI	**8.1** Asignar el ticket de creación de accesos privilegiados a los administradores de los sistemas de información donde se hayan solicitado dichos accesos.	Agente de Mesa de Ayuda	Tickets de Mesa de Ayuda
9. APROVISIONAR LOS ACCESOS PRIVILEGIADOS EN CADA PLATAFORMA SOLICITADA	**9.1** Teniendo en cuenta la solicitud recibida, los administradores procederán a asignar los accesos privilegiados en cada sistema solicitado.	Administradores de Sistemas de Información	Logs en sistemas de información
10. DOCUMENTAR EL FORMATO MATRIZ	**10.1** Una vez aprovisionados los privilegios, proceder a documentar el formato Matriz de Registro de Usuarios	Administradores de Sistemas de	Matriz de Registro de Usuarios

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO	Privilegiados y de Servicio en cada sistema de información donde se han otorgado los accesos. Continua en la actividad No. 26 para realizar el cierre de la solicitud inicial.	Información	Privilegiados y de Servicio
11. REALIZAR LA SOLICITUD DE CREACIÓN, MODIFICACIÓN O INACTIVACIÓN A TRAVÉS DE MESA DE AYUDA	**11.1** Realizar la solicitud de creación, modificación o inactivación del usuario no privilegiado correspondiente. Si la solicitud está relacionada con creaciones se debe adjuntar la documentación correspondiente como se indica en el Manual de Administración de Usuarios. **11.2** Realizar la solicitud de creación, modificación o eliminación de permisos de usuarios de red para acceder a la VPN Cliente a través de la mesa de ayuda integral.	Jefes de Área, Oficina de Contratación, Dirección de Talento Humano Jefe de la dependencia o coordinador del área	Ticket en mesa de ayuda, Formato de Administración de Usuarios Diligenciado Ticket en mesa de ayuda, Formato de creación, modificación o eliminación de VPN cliente
12. VERIFICAR TIPO DE SOLICITUD	**12.1.** El gestor de mesa de ayuda procederá con la verificación de la solicitud enviada.	Gestor de Mesa de Ayuda	Ticket en mesa de ayuda
13. ¿QUÉ TIPO DE SOLICITUD ES?	**13.1** ¿Qué tipo de solicitud se ha recibido por parte del solicitante? Creación – Ir a la actividad No. 14. Modificación – Ir a la actividad No. 18. Inactivación – Ir a la actividad No. 22	Gestor de Mesa de Ayuda	Ticket en mesa de ayuda
14. ASIGNAR A CADA ADMINISTRADOR DE SISTEMAS DE LA OTI SEGÚN LOS ACCESOS SOLICITADOS A LAS APLICACIONES	**14.1** El gestor de mesa de ayuda distribuye el ticket a cada uno de los gestores de aplicación para crear los permisos solicitados.	Gestor de Mesa de Ayuda	Ticket en mesa de ayuda
15. VALIDAR QUE LOS ACCESOS Y/O PERMISOS SOLICITADOS AL USUARIO ESTÉN ACORDES CON EL PERFIL SOLICITADO EN LA APLICACIÓN	**15.1** El administrador de cada sistema de información deberá revisar con base a su conocimiento y experiencia del sistema de información, si los permisos solicitados son pertinentes	Gestores de Aplicación	Tickets de Mesa de Ayuda
16. ¿ES PERTINENTE LA CREACIÓN DE LA SOLICITUD?	**16.1** ¿Es pertinente la solicitud de creación del usuario y sus permisos? **Si:** Ir a la actividad No. 17 **No:** Ir a la actividad No. 26, indicando la causal de rechazo correspondiente**.**	Gestores de Aplicación	Tickets de Mesa de Ayuda
17. CREAR LOS ACCESOS SOLICITADOS EN CADA PLATAFORMA	**17.1** Crear los usuarios y permisos en cada una de las plataformas correspondientes y luego ir a la actividad No. 26.	Gestores de Aplicación	Logs de Sistemas de Información
18. ASIGNAR A CADA ADMINISTRADOR DE SISTEMAS DE LA OTI SEGÚN LOS ACCESOS A MODIFICAR EN LAS APLICACIONES	**18.1.** El gestor de mesa de ayuda distribuye el ticket a cada uno de los administradores de los sistemas para realizar las modificaciones a los usuarios solicitados.	Gestor de Mesa de Ayuda	Tickets de Mesa de Ayuda
19. VALIDAR QUE LOS ACCESOS Y/O PERMISOS	**19.1.** El administrador de cada sistema de información deberá revisar con base a su conocimiento y experiencia del sistema de información, si la modificación de permisos es pertinente	Administradores de Sistemas de Información	Tickets de Mesa de Ayuda

ACTIVIDAD ESENCIAL DE VALOR No.	DESCRIPCIÓN DE ACTIVIDADES	CARGO O ROL DE PERSONA RESPONSABLE	CONTROL DE REGISTROS
A MODIFICAR SEAN ACORDES CON EL PERFIL, ÁREA Y APLICACIÓN SOLICITADO			
20. ¿SON PERTINENTES LAS MODIFICACIONES?	**20.1.** ¿Es pertinente la solicitud de modificación del usuario y sus permisos? **Si:** Ir a la actividad No. 21 **No:** Ir a la actividad No. 26, indicando la causal de rechazo correspondiente.	Administradores de Sistemas de Información	Tickets de Mesa de Ayuda
21. MODIFICAR LOS ACCESOS Y/O PERMISOS DEL USUARIO DE ACUERDO CON LA SOLICITUD	**21.1.** Modificar los permisos del usuario en cada una de las plataformas correspondientes y luego proceder con la documentación del caso en la actividad 26.	Administradores de Sistemas de Información	Logs de Sistemas de Información
22. ASIGNAR A CADA ADMINISTRADOR DE SISTEMAS DE LA OTI SEGÚN LOS ACCESOS A MODIFICAR EN LAS APLICACIONES	**22.1.** El gestor de mesa de ayuda distribuye el ticket a cada uno de los administradores de los sistemas para realizar la baja de los usuarios solicitados.	Gestor de Mesa de Ayuda	Tickets de Mesa de Ayuda
23. REALIZAR LA INACTIVACIÓN DE USUARIOS EN TODOS LOS SISTEMAS DE INFORMACIÓN Y ELIMINAR LOS PRIVILEGIOS EN CADA SISTEMA	**23.1.** El administrador de cada sistema de información deberá revisar el sistema de información y realizar la eliminación de los permisos e inactivación de la cuenta.	Administradores de Sistemas de Información	Logs de los Sistemas de Información
24. ¿QUÉ TIPO DE USUARIO SE HA SOLICITADO INACTIVAR?	**24.1.** ¿Qué tipo de usuario se ha solicitado inactivar? Privilegiado / Servicio: Ir a la actividad No. 25 No privilegiado: Ir a la actividad No. 26	Administradores de Sistemas de Información	Logs de los Sistemas de Información
25. ACTUALIZAR EL FORMATO MATRIZ DE REGISTRO DE USUARIOS PRIVILEGIADOS Y DE SERVICIO.	**25.1.** Actualizar el formato Matriz de Registro de Usuarios Privilegiados y de Servicio en cada sistema de información donde se han eliminado los accesos.	Administradores de Sistemas de Información	Matriz de Registro de Usuarios Privilegiados y de Servicio
26. DOCUMENTAR EL CORREO ELECTRÓNICO O CASO EN MESA DE AYUDA	**26.1.** Realizar la documentación del correo electrónico o el caso en mesa de ayuda con la gestión o rechazo realizado por parte del personal de la OTI.	Personal Oficina de Tecnologías de la Información	Ticket de Mesa de Ayuda Correo Electrónico
27. ORGANIZACIÓN DE DOCUMENTOS **FIN**	**27.1** Organizar los documentos en el archivo digital de la OTI de la SNR. Cargar en el repositorio definido para tal fin.	Personal Oficina de Tecnologías de la Información	Documentos del proceso. Repositorio.

4. DOCUMENTOS ASOCIADOS:

Documentos que hacen parte del procedimiento

4.1. Documentos internos:

Manual de Gestión de Usuarios y Contraseñas Formato para Administración de Usuarios
Formato Matriz de Registro de Usuarios Privilegiados y de Servicio
Formato de creación y/o asignación de permisos a buzones genéricos.
Formato de creación, modificación o eliminación de VPN cliente

4.2. Documentos externos: No aplica.

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
GTI-PR-007	1	03/Oct./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.
GTI-PR-007	2	20/Ago./2026	Se adiciona al procedimiento la política de operación y actividad relacionada con la gestión de los buzones genéricos de las cuentas de correo electrónico. Se incorpora al procedimiento la política de operación y actividad relacionada con la solicitud de creación, modificación o eliminación de permiso de acceso a la red mediante VPN.

ELABORACIÓN, REVISIÓN Y APROBACIÓN		
ELABORÓ	**REVISÓ**	**APROBÓ**
Oscar Fabián Corredor Camargo Jorge Armando Serrano Caicedo	Alirio Tovar Castellanos	Jorge Arcecio Cañaveral Rojas Nubia Patricia López Méndez
Coordinador Grupo de Servicios Tecnológicos Profesional Especializado Oficina de Tecnología de la Información	Contratista Oficina Asesora de Planeación	Jefe de Oficina de Tecnologías de la Información Jefe de la Oficina Asesora de Planeación
Fecha: 20/08/2026	Fecha: 20/08/2026	Fecha: 20/08/2026