

	PROCEDIMIENTO	ADMINISTRACIÓN DE CUENTAS DE USUARIO Y ACCESO A LOS RECURSOS TECNOLÓGICOS	CÓDIGO	ADMS-P-014
	ACTIVIDAD	SOPORTE DE SERVICIOS ADMINISTRATIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN	VERSIÓN	6
	PROCESO	ADMINISTRACIÓN DE BIENES Y SERVICIOS	FECHA	20/09/2023
OBJETIVO	Orogar o revocar a los colaboradores de la Agencia Nacional de Tierras, los permisos y privilegios de autenticación para el control de acceso lógico a los sistemas de información de la Agencia.			
ALCANCE	Este procedimiento inicia con la solicitud de creación y/o novedad de usuario y termina con la respuesta a la solicitud.			
RESPONSABLE	Secretaría General - Equipo de Infraestructura y Soporte Tecnológico, Dirección de Gestión del Ordenamiento Social de la Propiedad, Subdirección de Sistemas de Información			

1. DEFINICIONES (Términos y Siglas)

<p>Autenticación: es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores.</p> <p>Autorización: el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.</p> <p>ANT: Agencia Nacional de Tierras.</p> <p>ArcGIS: Conjunto de productos de software de información geográfica ó Sistema de Información Geográfica.</p> <p>Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.</p> <p>Caso o ticket: es un identificador o dato numérico contenido y generado por la mesa de servicios que contiene información acerca de las necesidades requeridas por un usuario final en busca de asesoría, información o soporte técnico.</p> <p>Contraseña o clave: es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso.</p> <p>Directorio Activo: es una herramienta tecnológica que proporciona un servicio ubicado en uno o varios servidores para crear objetos como usuarios, equipos o grupos para administrar las credenciales durante el inicio de sesión de los equipos que se conectan a una red.</p> <p>EIST: Equipo de Infraestructura y Soporte Tecnológico.</p> <p>Grupo: agrupación de usuarios que tienen los mismos niveles de acceso sobre determinados archivos o carpetas.</p> <p>Mesa de servicios de TI: es el punto de contacto a través del cual los usuarios interactúan con TI a través de la gestión de incidentes, solicitudes, requerimientos y problemas relacionados con la tecnología, infraestructura y comunicaciones informáticas, que permiten satisfacer las necesidades permanentes de los usuarios.</p> <p>Nombre de usuario: ¿es la respuesta a la pregunta "quién es usted?". Como tal, los nombres de usuarios tienen un requerimiento principal, deben ser únicos. En otras palabras, cada usuario debe tener un nombre de usuario que sea diferente a todos los otros usuarios en ese sistema.</p> <p>Permiso: poder que se otorga a los usuarios y grupos de usuarios sobre los archivos, carpetas, directorios entre otros.</p> <p>Privilegio: es la delegación de autoridad sobre un sistema informático y permite a un usuario realizar unas tareas específicas.</p> <p>Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).</p> <p>Sistema de información: son aquellos componentes que ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.</p> <p>SIT: Sistema Integrado de Tierras.</p> <p>Solicitud: es una petición formal de un usuario pidiendo información, asesoramiento, un cambio estándar o acceso a un servicio tecnológico.</p> <p>TI: Abreviatura de Tecnología de la información.</p> <p>VPN: Virtual Private Network - Red Privada Virtual.</p>
--

2. GENERALIDADES

Los conceptos de este documento se apoyan en:

Sistema de Gestión de Seguridad de la Información ISO 27001.
Modelo de Seguridad y Privacidad de la Información (MSPI).

3. RIESGOS Y CONTROLES ASOCIADOS AL PROCEDIMIENTO

A partir del análisis de los riesgos que pueden afectar el cumplimiento de los objetivos de los procesos, la Oficina de Planeación orienta a las dependencias en la identificación de las tareas críticas de sus procedimientos en las que se puede materializar un riesgo y el establecimiento de las correspondientes tareas de control preventivo, detectivo o correctivo.

Para facilitar la identificación de las tareas críticas y las correspondientes tareas de control, el procedimiento presenta el siguiente método de señalización:

Tareas Críticas	Son las tareas donde se puede materializar un riesgo que impacte negativamente el logro del objetivo del procedimiento. En la matriz de desarrollo del procedimiento y en el diagrama de flujo se identifican tareas críticas con texto en color rojo y con el símbolo ☹
Tareas de Control	Son las tareas que permiten prevenir o corregir el impacto de los riesgos en el logro del objetivo del procedimiento. En la matriz de desarrollo del procedimiento y en el diagrama de flujo se identifican tareas de control con texto en color azul y con el símbolo ☺

4. DESARROLLO DEL PROCEDIMIENTO

No	Tarea	Descripción	Tiempo de Ejecución	Responsable
1	Solicitar creación y/o novedad de usuario	Realizar a través de la Mesa de Servicios de TI, el registro de la solicitud adjuntando la forma ADMS-F072 diligenciada en su totalidad y copia del contrato o acta de posesión. Si el Colaborador requiere acceso VPN para el cumplimiento de sus funciones también deberá diligenciar la Forma ADMS-F-078 . A través de la Mesa de Servicios de TI, se enviará notificación automática del registro con el número de caso (Ticket) asignado para que el usuario realice el seguimiento y control de la solicitud. Nota: Para la creación de los usuarios del Sistema Integrado de Tierras SIT de los funcionarios, contratistas y/o colaboradores externos que apoyan la misionalidad de la Agencia Nacional de Tierras a través de contratos interadministrativos, se deberá utilizar la Forma ADBMS-F-073 y se deberá diligenciar y firmar el acuerdo de confidencialidad INTI-F-011 . ADMS-F-072 FORMA CREACIÓN Y/O NOVEDAD DE USUARIOS ADBMS-F-073 FORMA CREACIÓN Y/O NOVEDAD DE USUARIOS EN EL SISTEMA INTEGRADO DE TIERRAS - SIT ADMS-F-078 SOLICITUD DE VPN USUARIOS INTERNOS Y EXTERNOS INTI-F-011 ACUERDO DE CONFIDENCIALIDAD		Dependencias ANT
2	Recibir y validar la solicitud	Recibir y validar que el usuario solicitante este autorizado para este trámite. Si está autorizado, se asigna a un analista para su gestión y queda en estado "Asignado" si no, se cambia la categoría a "Informativo" y se gestiona el caso indicando el motivo por el cual no se puede dar trámite al requerimiento, así mismo, deberá relacionar en la respuesta a la(s) personas autorizadas en la dependencia correspondiente para realizar la solicitud a través de la Mesa de Servicio de TI.		Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)

3	Atender la solicitud	<p>Atender el caso a través de la mesa de servicios de TI por parte del analista y revisar si contiene la documentación necesaria para atender el caso.</p> <p>Si se trata de una creación de usuario se deberá validar la siguiente información:</p> <ol style="list-style-type: none"> 1) Forma ADMBS-F-072 debidamente diligenciada. 2) Si es funcionario, la resolución de nombramiento. 3) Contrato de prestación de servicios si es contratista. 4) Forma ADMBS-F-078 debidamente diligenciada (si aplica). <p>Si es una novedad, revisar que la Forma ADMBS-F-072 este completamente diligenciada.</p> <p>En el caso que la necesidad sea crear un usuario el analista debe continuar con la tarea No. 4, si la necesidad es una novedad de usuario deberá continuar con la tarea No. 5.</p> <p>Nota: Si se requiere crear o activar un usuario en el aplicativo SIT, el analista revisará que el usuario se encuentra creado en el directorio activo y procederá a crear el caso SIT, lo asignará al responsable de la Subdirección de Sistemas de Información de Tierras, quien validará que el usuario solicitante este autorizado para este trámite y revisará si contiene la documentación debidamente diligenciada para atender el caso (ADMBS-F-073 E INTI-F-011)</p> <p>ADMBS-F-072 FORMA DE CREACIÓN Y/O NOVEDAD DE USUARIOS ADMBS-F-073 FORMA CREACIÓN Y/O NOVEDAD DE USUARIOS EN EL SISTEMA INTEGRADO DE TIERRAS - SIT V2 ADMBS-F-078 SOLICITUD DE VPN USUARIOS INTERNOS Y EXTERNOS INTI-F-011 ACUERDO DE CONFIDENCIALIDAD</p>
4	<p>Ⓢ</p> <p>Crear usuario</p>	<p>Crear el nuevo usuario teniendo en cuenta el Instructivo ADMBS-I-009. Adicionalmente, se deberán diligenciar los siguientes datos en el directorio activo:</p> <ol style="list-style-type: none"> 1) Nombres y apellidos completos 2) Cargo y descripción del cargo 3) Grupo al que pertenece 4) Departamento (oficina) 5) Número de teléfono de contacto y extensión 6) Correo electrónico de la Agencia (previa creación del usuario) 7) Página web de la Agencia 8) Dirección de la sede donde ejecutará sus labores 9) Ciudad 10) Número de la cédula 11) País 12) Aplicar la política para que el usuario cuando ingrese por primera vez, cambie su clave. 13) Si el colaborador es contratista se debe diligenciar la fecha de terminación del contrato para que el sistema lo inactive de forma automática una vez finalice. <p>Nota 1: Si la cuenta es genérica se realiza el mismo proceso identificando a la persona responsable para el manejo de la misma. Se aclara que la únicas cuentas utilizadas para la distribución masiva de correos electrónicos son: Secretaría General, Oficina de comunicaciones, Talento Humano y Equipo de Infraestructura y Soporte Tecnológico. El resto de dependencias deberán hacer uso del servicio "divulgación masiva" de la mesa de servicios de TI.</p> <p>Nota 2: Los usuarios de administración de bases de datos y servidores deberán ser diferentes a las cuentas propias asignadas a cada colaborador.</p> <p>ADMBS-I-009 NOMBRAMIENTO DE USUARIOS Y ASIGNACIÓN DE CONTRASEÑAS</p>
5	<p>Ⓢ</p> <p>Identificar novedad de Usuario</p>	<p>Identificar el tipo de novedad que trata la solicitud:</p> <p>Inactivación de usuario, esto se puede presentar debido a:</p> <ol style="list-style-type: none"> 1) El Colaborador ya no trabaja en la agencia. 2) Finalización del contrato de prestación de servicios. 3) El Colaborador esta en periodo de vacaciones o de licencia. 4) El Colaborador se encuentra suspendido temporalmente. 5) La cuenta es genérica y ya no se usa. 6) Otras causales. <p>Activación de usuario, esta situación se presenta cuando:</p> <ol style="list-style-type: none"> 1) El usuario ya existía y se realizó una nueva contratación. 2) El usuario asignado al colaborador fue inactivado por las causales 3, 4, 5 y 6 antes mencionadas y se deben activar <p>Nota 1: Las novedades de los funcionarios y contratistas deben ser reportadas por la Subdirección de Talento Humano y el Grupo Interno de Trabajo de Gestión Contractual según corresponda, una vez se presente la novedad a través de la mesa de servicios de TI.</p> <p>Modificación de usuario, se puede presentar por:</p> <ol style="list-style-type: none"> 1) Cambio de cargo o dependencia. 2) Cambio o asignación de responsabilidades. 3) Ajuste de usuario por errores ortográficos involuntarios. <p>Nota 2: Las solicitudes de activación de usuarios y/o cambios de contraseñas deberán quedar registradas en la mesa de servicios de TI por parte de los Directores, Secretario General, Subdirectores, Asesores de Dirección General, Jefes de Oficina o en dado caso, el/la asistente de cada uno de ellos.</p>
6	Asignar privilegios	<p>Asignar los perfiles para el acceso autorizado a los diferentes sistemas de información de la entidad, una vez creada la cuenta o realizada la novedad del usuario y previa validación de las necesidades de acceso a las aplicaciones de la Agencia previstas en la Forma ADMBS-F-072.</p> <p>En el caso que se requieran permisos de administrador porque su rol lo demanda, deberá escalarlo a segundo nivel continuando con la tarea No. 7, de lo contrario continua con tarea No. 8.</p> <p>ADMBS-F-072 FORMA DE CREACIÓN Y/O NOVEDAD DE USUARIOS</p>
7	Escalar a segundo nivel	<p>Verificar si el caso no pudo otorgar los permisos y/o perfiles requeridos en primer nivel para que este sea escalado al segundo nivel, con el fin de habilitar los accesos necesarios y dar respuesta a la solicitud.</p>

1 día

<p>Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)</p> <p>Subdirección de Sistemas de Información de Tierras</p>
<p>Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)</p>
<p>Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)</p> <p>Subdirección de Talento Humano</p> <p>Grupo Interno de Gestión Contractual</p>
<p>Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)</p>
<p>Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)</p> <p>Subdirección de Sistemas de Información de Tierras</p>

8	Responder la solicitud	<p>Dar respuesta a la solicitud a través de la mesa de servicios de TI indicando:</p> <ol style="list-style-type: none"> 1) Nombre de usuario. 2) Clave asignada. 3) Recomendación de cambio de clave al inicio de sesión. 4) Aplicaciones autorizadas. 5) Link de acceso al apartado de creación del carnet digital. 6) Link de acceso al formulario de solicitud de licencias ARCGIS (si aplica). <p>Finalmente, el caso pasa a estado "ejecutado" y se envía la respuesta de la solución al solicitante.</p>	Secretaría General (Equipo de Infraestructura y Soporte Tecnológico)
---	------------------------	---	--

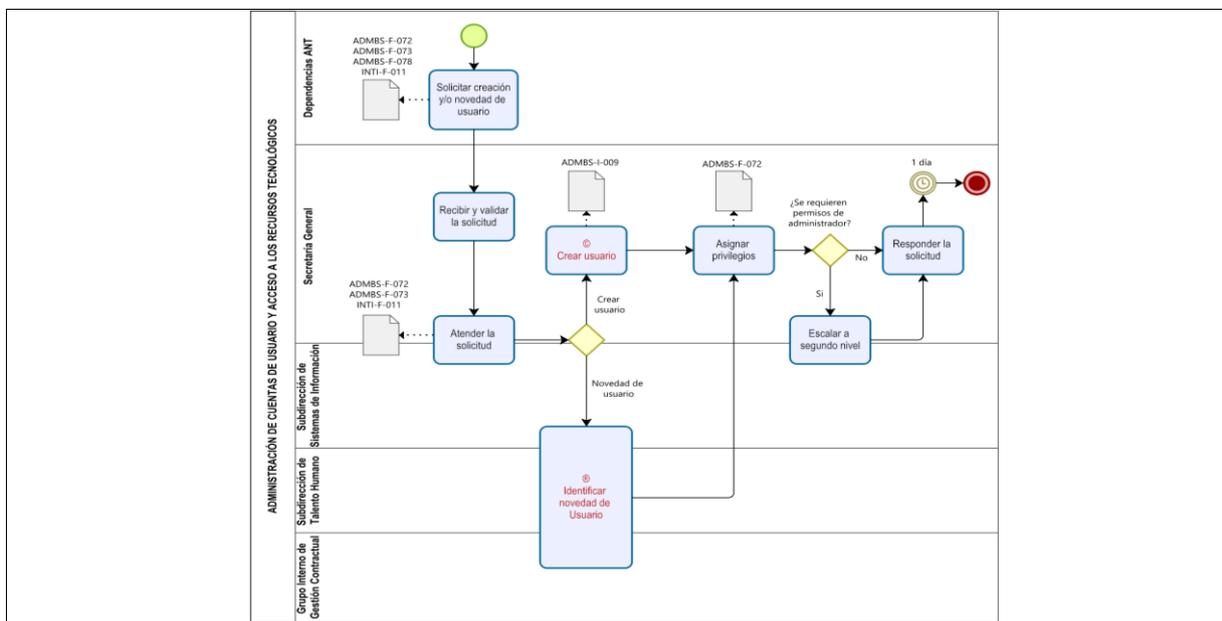
5. NORMATIVIDAD APLICABLE

Ley 1341 de 2009: Se definen principios y conceptos sobre la información y la organización de las tecnologías de la información y las comunicaciones -TIC.
Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública.
Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015: Decreto único reglamentario del Sector de Tecnologías de Información y Comunicaciones.
Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 del 2014 y se dictan otras disposiciones.
Decreto 415 de 2016: Definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones (Departamento Administrativo de la Función Pública).
Decreto 1008 del 14 de junio de 2018: 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.

6. DOCUMENTOS ASOCIADOS

ADMBS-F-072 FORMA CREACIÓN Y/O NOVEDAD DE USUARIOS.
 ADMBS-F-078 SOLICITUD DE VPN USUARIOS INTERNOS Y EXTERNOS
 ADMBS-F-073 FORMA CREACIÓN Y/O NOVEDAD DE USUARIOS EN EL SISTEMA INTEGRADO DE TIERRAS - SIT V2
 INTI-POLITICA-001 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.
 INTI-POLITICA-008 LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA ANT.
 INTI-F-011 ACUERDO DE CONFIDENCIALIDAD
 ADMBS-I-009 NOMBRAMIENTO DE USUARIOS Y ASIGNACIÓN DE CONTRASEÑAS.

7. DIAGRAMA DE FLUJO



ELABORÓ	Irma Irene Cuello González	REVISÓ	Roberto Andrés Zabala Barrera	APROBÓ	Daniel María Medina Gonzalez
CARGO	Contratista - Secretaría General - Equipo de Infraestructura y Soporte tecnológico	CARGO	Contratista - Secretaría General - Equipo de Infraestructura y Soporte tecnológico	CARGO	Secretario General
FIRMA	ORIGINAL FIRMADO	FIRMA	ORIGINAL FIRMADO	FIRMA	ORIGINAL FIRMADO
FECHA	14/08/2023	FECHA	18/08/2023	FECHA	13/09/2023



La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia. La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.



INTI-F-002 Versión 3 4-mar.-19