ADMINISTRACIÓN DE USUARIOS Y/O CONTRASEÑAS			
PROCESO:	GESTIÓN TICs		
PROCEDIMIENTO:	ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA		
FECHA DE APROBACIÓN:	**CÓDIGO:**	**VERSIÓN:**	**PÁGINA:**
15/07//2026	GTI02-GUI02	02	**1** de **11**

1. OBJETIVO

Establecer mecanismos que permitan asegurar el cumplimiento de requisitos mínimos de robustez y protección de contraseñas para garantizar la trazabilidad y registro de todas las operaciones del ciclo de vida de las cuentas de usuario, así como seguir la misma secuencia de actividades para la creación o baja de usuarios.

2. ALCANCE

La presente guía aplica a todos los funcionarios, contratistas, administradores y terceros que hagan uso de los servicios de TI relacionados en el catálogo de servicios de TI, y será aplicada al control de acceso lógico de los siguientes componentes tecnológicos que integran los servicios de TI, sin limitarse a estos:

- Administración de Infraestructura (servidores, almacenamientos, switches y seguridad)
- Administración de los servicios de TI y tecnológicos
- Administración componentes centro de datos (UPS, AA, extinción y detección de incendios, control de acceso)
- Servicios colaborativos y de nube
- Plataformas de respaldo y restauración de información
- Administración de las capas de las aplicaciones y sistemas de información.
- Servicios de seguridad de usuario, perimetral y aplicación
- Equipos tecnológicos de oficina
- Administración de servicios Cloud (IaaS, SaaS,PaaS)

3. DEFINICIONES

- **Id (identificación de usuario)**: conjunto de caracteres alfanuméricos que identifica a un usuario.
- **Cuenta de usuario**: se entiende por cuenta de usuario, al Id de usuario y su contraseña asociada que le permiten ingresar de forma autorizada a los servicios de TI.
- **Perfil**: conjunto de permisos o funciones que puede realizar un usuario en un servicio de TI; los perfiles se asocian a las cuentas de usuario.
- **Administradores técnicos**: rol asignado a los colaboradores del GIT de Apoyo Informático, de acuerdo con las funciones del cargo u obligaciones del contrato, así como, a los responsables de los diferentes servicios de TI y tecnológicos.
- **Cuenta privilegiada:** es aquella que posee permisos o niveles de acceso superiores a los de un usuario estándar tanto en un sistema informático, red o aplicación y a los distintos servicios de TI.
- **Cuenta de servicio:** es una cuenta creada para permitir que una

aplicación, sistema o servicio informático ejecute procesos automatizados o acceda a recursos en una infraestructura tecnológica y no están asociadas a una persona.

- **Break-glass:** es un mecanismo de acceso de emergencia que permite a usuarios autorizados obtener privilegios especiales o acceder temporalmente a sistemas, aplicaciones o datos críticos en situaciones excepcionales.
- **Acceso JIT:** el acceso Just-In-Time (JIT) es un mecanismo de seguridad que otorga a los usuarios privilegios elevados de manera temporal y controlada, solo cuando son necesarios para realizar una tarea específica.
- **Colecciones en Bóveda de contraseñas:** es un conjunto de elementos o contraseñas, llaves API, notas seguras o información de acceso que se agrupan y comparten entre los miembros de una organización o equipo.
- **Objeto de Directiva de Grupo – GPOs**: es una característica de Microsoft Windows en Active Directory que permite la administración centralizada y configuración de sistemas operativos, aplicaciones y usuarios

4. RESPONSABLES DE CUMPLIMIENTO

Esta guía es responsabilidad de todos los administradores de los servicios de TI y sus componentes tecnológicos, así como de los funcionarios, contratistas y colaboradores de la Contaduría General de la Nación (CGN), y de terceros que accedan o hagan uso de los recursos tecnológicos institucionales.

Responsabilidades:

- El propietario del activo ejercerá la función de aprobador de los privilegios asociados a su activo.
- El GIT de Apoyo Informático actuará como custodio de las cuentas privilegiadas y velará por su correcta administración.
- El Equipo de Seguridad de la Información será responsable de realizar revisiones periódicas para verificar el cumplimiento de los controles establecidos en la presente guía.

5. GESTIÓN DE CUENTAS

5.1 Creación y aprobación

Para el ingreso de un usuario a los diferentes sistemas de información se debe crear la solicitud en la herramienta de mesa de servicios, previo diligenciamiento del formato GTI010-FOR 09 Gestión de Cuentas De Usuario, el cual deberá ir adjunto a dicha solicitud.

Para el primer ingreso a los diferentes sistemas, el responsable de asignar las cuentas de acceso a las aplicaciones o sistemas de información proporcionará a cada usuario una contraseña. En algunos casos se crea la cuenta de usuario y se asigna directamente una contraseña, mientras que en otros se entrega una contraseña temporal donde el sistema solicitará cambiar de manera inmediata en el primer acceso.

5.2 Identificación y nomenclatura

Como norma general, para todos los ID de usuario que requieran acceso a los servicios de TI clasificados como misionales, de gestión o de apoyo, se utilizará la inicial del primer nombre y apellido del usuario. Por ejemplo, Juan Fernando Pérez Campo tendrá el ID: *jperez*."

Para los nombres y apellidos compuestos se tomará la inicial del primer nombre y apellido. En caso de que ya exista un usuario con la misma identificación, se emplearán las iniciales del primer y segundo nombre junto con el apellido; por ejemplo, si 'jperez' ya está asignado, el nuevo usuario será 'jfperez'. Si la persona no tiene segundo nombre, se utilizará la inicial del segundo apellido; por ejemplo: 'jperezc'.

La asignación de usuarios para acceso a un recurso tecnológico tendrá en cuenta los siguientes criterios:

- El usuario será el mismo a través de todos los sistemas, ambientes y/o máquinas donde deba acceder.
- Los nombres de usuario siempre serán en minúsculas.
- El nombre es asignado por el responsable del componente tecnológico, y será la "identificación" del usuario para el de inicio de sesión al componente tecnológico.
- El Id del usuario tendrá una longitud mínima de 4 (cuatro) caracteres y una longitud máxima de 15 (quince) caracteres.

5.3 Restricciones de uso y privilegios

Se debe asegurar que solo usuarios, componentes y servicios autorizados dispongan de privilegios elevados, y que su asignación, uso, monitoreo y revocación se gestionen bajo el principio de menor privilegio y segregación de funciones.

El numeral cubre cuentas de administrador y root, administrador de dominio, administrador glogal para (SaaS/IaaS/PaaS), consolas de seguridad, hipervisores,

bases de datos, endpoints con elevación, dispositivos de red, cuentas de servicio y "break-glass", tanto on-premise como nube.

Cuenta privilegiada: cuenta con capacidades que pueden afectar la confidencialidad, integridad o disponibilidad del sistema o información.

Cuenta de servicio: identidad técnica utilizada por aplicaciones/tareas automatizadas.

Cuenta "break-glass": credencial de emergencia guardada en vault para continuidad operativa de uso excepcional y auditada.

PAM (Privileged Access Management): soluciones/controles para bóveda de credenciales, session recording, password rotation y acceso JIT (Just in Time).

- Roles y responsabilidades

Solicitante: justifica necesidad y tiempo de uso.
Aprobador (Propietario del activo / líder del proceso): valida la necesidad de privilegios.
Custodio (GIT de Apoyo Informático): crea, configura, monitorea y revoca.
Seguridad de la Información: revisa evidencias, registros y cumplimiento.

Autorización formal y trazable: todo permiso, modificación o revocación de privilegios se solicita por mesa de servicio (GTI010-FOR 09) con doble validación "Solicitante + Aprobador". No se asignan privilegios por correo/chat.

Menor privilegio y tiempo limitado (JIT): los privilegios serán lo mínimo y por el menor tiempo posible; se prefieren roles/grupos sobre asignaciones directas a usuarios.

Segregación de funciones: los administradores de plataformas, seguridad, BD y redes no deben compartir funciones en conflicto sin compensaciones (revisión independiente, peer review).

Controles de autenticación reforzados: MFA obligatorio para todo acceso privilegiado; prohibido el acceso privilegiado desde equipos no gestionados.

Cuentas de servicio: Deben: (i) tener propietario asignado; (ii) no iniciar sesión interactiva; (iii) usar secrets rotados; (iv) documentar su uso, alcance y dependencias.
PRETESH BISWAS

Break-glass: las credenciales de emergencia se custodian en vault (ya contemplado en "Almacenamiento") y su uso queda registrado y revisado en 24 h.

Monitoreo y registro: toda sesión privilegiada debe dejar trazas: quién, qué, cuándo y desde dónde; se habilita grabación de sesiones donde la tecnología lo permita y se revisan al menos mensualmente.
Revisión periódica: los privilegios se revisan trimestralmente (o ante cambios de rol/salida), con evidencia de ajuste o revocación. Excepciones requieren aprobación formal y fecha de expiración.

Restricciones de uso: con privilegios no se navega por Internet, no se leen correos, no se instala software no autorizado, y se prohíbe el reuso de contraseñas entre entornos. (Mantiene coherencia con la sección de contraseñas y protección ya vigente).

Bóveda y rotación de credenciales: las credenciales privilegiadas se guardan en bóveda autorizada con rotación tras uso, caducidad o incidente.

Alta/Baja: la baja de privilegios es inmediata ante desvinculación o cambio de funciones; se alineará con el procedimiento de BAJA DE USUARIO y notificación de Talento Humano/Servicios Generales.

Evidencias mínimas: solicitudes y aprobaciones (mesa de servicio), membresías de grupo/roles, bitácoras de cambios, registros de sesión, reportes de revisión trimestral, actas de uso "break-glass".

5.4 Contraseñas, claves y custodia

5.4.1 Parámetros generales de las contraseñas:

a) Toda contraseña debe tener por lo menos una combinación de caracteres alfanuméricos, mayúsculas, minúsculas y caracteres especiales, (p.ej. >:;.,<\+*/=(){}[]!¡¿?"#%|$&°~¬@_-).
b) Toda contraseña debe tener una longitud mínima de doce (12) caracteres y se recomienda un máximo de hasta 30.
c) No está permitida el uso de secuencias de teclado (p.ej. "qwerty", "asdf" o las típicas en numeración: "1234")
d) No se debe usar referencias comunes, como el nombre del servidor, del usuario u otros similares.
e) La contraseña actual no debe ser igual en su estructura (p. ej. p1: Juan01admin, p2: Juan02admin) a ninguna de las últimas 5 contraseñas utilizadas. Esto se debe garantizar por Objeto de Directiva de Grupo - GPOs por parte del administrador del controlador de dominio.

f) No escribir la contraseña en un papel o documento donde quede al alcance de otra persona. Tampoco se deben guardar en documentos de texto dentro del propio computador o dispositivo (p.ej. no guardar las contraseñas de los correos y recursos tecnológicos en documentos de texto dentro del computador o en el teléfono móvil).

g) Siempre se deben cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes inmediatamente luego de ingresar por primera vez al sistema.

h) No utilizar la característica de "Recordar Contraseña" existente en las aplicaciones y/o navegadores de internet

5.4.2 Doble factor de autenticación

a) Para fortalecer el acceso a varios de los servicios de TI se aplica la configuración de doble factor de autenticación (2FA).

b) El método de doble factor de autenticación consiste en ingresar la contraseña seguido de un código que recibirá el usuario a su dispositivo móvil, verificando que sea realmente el dueño de la cuenta o por medio de la aplicación autenticadora que disponga el usuario.

c) El uso de cuentas privilegiadas requiere doble factor de autenticación (**2FA) o** múltiple factor de autenticación **(MFA), rotación** tras uso en tareas de alto impacto y prohibición de "recordar contraseña" en navegadores y/o aplicaciones.

5.4.3 Cambio de contraseña para usuarios

Cuando el usuario inicie la sesión en un servicio de TI asociado al controlador de dominio con su Id (p.ej. agarcia), aparecerá un mensaje indicando que su contraseña está próxima a caducar o en su defecto, llegará un mensaje de correo electrónico indicando que debe realizar el respectivo cambio. Esta guía esta implementada en el Objeto de Directiva de Grupo - GPO para que se aplique cada 60 días.

Tanto para los usuarios en sitio como para los que están fuera de la CGN (teletrabajo o trabajo en casa) y conectados a VPN, podrán hacer el cambio de la contraseña en el aplicativo web suministrado por la entidad.

El usuario puede hacer rotación de contraseña en el momento que lo desee siempre y cuando cumpla con las indicaciones de contraseña segura indicadas en el aplicativo.

5.4.4 Cambio de contraseña para administradores

a) El cambio de contraseña será necesario para usuarios con privilegios de administradores.

b) Realizar cambio de contraseña de cuentas de administración genéricas al asignarse al administrador encargado y en caso de su retiro.

c) Las contraseñas deben cambiarse con una periodicidad entre uno y tres meses, durante los primeros cinco (5) días hábiles, lo cual es responsabilidad de cada uno de los administradores de hardware o software que le competa. En el caso de las cuentas de usuarios de redes sociales se debe realizar el cambio cada tres (3) meses.

5.4.5 Custodia: almacenamiento seguro (Bóveda de contraseñas)

Se debe asegurar que todas las credenciales se almacenen, usen y roten de forma segura en la bóveda de la entidad, con trazabilidad, mínimo privilegio y controles de acceso reforzados.

Principios generales

a) Repositorio único**:** todas las contraseñas de administración (infraestructura, aplicaciones, bases de datos, red, nube, consolas de seguridad, cuentas de servicio y "break-glass") deben guardarse en la bóveda de contraseñas; se prohíbe su almacenamiento en papel, planillas, correos o navegadores.
b) Cifrado y MFA**:** acceso a la bóveda obligatoriamente con MFA y desde equipos gestionados.
c) Menor privilegio y segregación**:** accesos a través de colecciones/grupos por rol y sistema; no se comparten credenciales fuera de la bóveda.
d) Trazabilidad: toda visualización, copia o descarga genera registro de auditoría y debe estar asociada a una solicitud de la mesa de servicio (solicitud/aprobación).
e) Compartir: se podrán compartir las colecciones con grupos o usuarios

Registro estándar por credencial (campos obligatorios)

Cada entrada en la bóveda de contraseñas debe contener, como mínimo:

- **Recurso administrado:** (ej. *SKYLAB* / URL del sistema)
- **Cuenta/ID de usuario:** (respetando **mayúsculas/minúsculas** – *case sensitive*)
- **Secreto/Clave** (guardado solo en la bóveda, nunca en texto plano fuera de ella)
- **Propietario del activo / Aprobador**

- **Clasificación de la información** (ej. Restringida)
- **Evidencia de solicitud** (ID de ticket)
- **Política de rotación** (frecuencia/condiciones)
- **Estado de MFA en el sistema destino** (habilitado/pendiente)
- **Fecha de último cambio** y **próxima rotación**
- **Notas técnicas** (alcance, dependencias, restricciones)

Ejemplo (en bóveda):

Recurso: *SKYLAB (https://skylab.local/admin)*
Cuenta: *root*
Propietario/Aprobador: *[Nombre/Rol]*
Ticket: *001234*
Rotación: *60 días o tras baja de personal/incidente*
MFA: *Habilitado en sistema*
Último cambio: *2025-05-30* | Próximo: *2025-08-28*

Creación, consulta y rotación (flujo)

a) **Solicitud:** el administrador o responsable **solicita** alta/consulta/rotación mediante **mesa de servicio**, justificando alcance y vigencia.
b) **Aprobación:** el **Propietario del activo** aprueba; Seguridad revisa si aplica.
c) **Ejecución:** el **Custodio (GIT de Apoyo Informático)** crea/actualiza la entrada en la **colección** correspondiente y **rota** credenciales en el sistema destino.
d) **Cierre y evidencia:** se adjuntan **registros de auditoría** (bóveda y sistema), se actualizan **fechas de rotación** y se cierra la solicitud.

Acceso y custodia

- **Accesos** a credenciales privilegiadas sólo para **grupos/roles autorizados** (colecciones).
- **Prohibido** copiar claves fuera de la bóveda; si por operación se revela una clave, **debe rotarse** al finalizar la tarea.
- **Revisión trimestral** de membresías de colecciones y de accesos a entradas privilegiadas.

Respaldo y continuidad

- **Backups cifrados** de Vaultwarden al repositorio corporativo (al menos **diarios**), con copia adicional en medio seguro.
- **Prueba de restauración** semestral documentada.

- **Exportaciones** desde la bóveda sólo por el **equipo custodio**, cifradas y asociadas a solicitud.

"Break-glass" (uso excepcional)

- Se mantiene **una credencial de emergencia** por sistema crítico (o clave maestra de recuperación según aplique), **custodiada en bóveda de contraseñas**.
- **La clave de recuperación maestra**. se comparte a 3 administradores designados por el Coordinador del GIT de Apoyo Informático en el aplicativo de la bóveda de contraseñas para la gestión de todas las contraseñas de los servicios de TI y sus componentes.
- **Uso excepcional**, sólo ante incidentes que comprometan **confidencialidad, integridad o disponibilidad**; todo acceso **se registra** y se **rota** la credencial **dentro de las 24 horas** posteriores.

Privilegios de acceso: tendrán acceso adicional a todas las contraseñas de los administradores y sistemas informáticos el coordinador del GIT de Apoyo Informático y quien el designe en caso de ausencia del responsable del componente tecnológico.

Prohibiciones y controles complementarios

- Prohibido el **autoguardado en navegadores** o gestores personales.
- Prohibido **reenviar** credenciales por correo/chat.
- En tareas con privilegios elevados no se debe: navegar por Internet, leer e-mail o instalar software no autorizado.
- Cualquier incumplimiento deberá reportarse como **incidente de seguridad**.

5.4.5 Registro y monitoreo

Toda sesión privilegiada debe dejar trazas: quién, qué, cuándo y desde dónde; se habilita grabación de sesiones donde la tecnología lo permita y se revisan al menos mensualmente.

5.4.6 Revisión periódica y desactivación de usuarios

Revisión periódica**:** los privilegios se revisan trimestralmente (o ante cambios de rol/salida), con evidencia de ajuste o revocación. Excepciones requieren aprobación formal y fecha de expiración.

Baja de un usuario**:** cuando un empleado se desvincule de la entidad,

inmediatamente se reciba la información, el responsable del componente procederá a la inactivación del usuario en los respectivos componentes tecnológicos a los cuales tuviere acceso el usuario.

Aclaración: los usuarios en los diferentes componentes tecnológicos no se eliminan por razones de auditoría y seguimiento a usuarios, por el contrario, son inactivados.

Nota: El GIT de Talento Humano y el GIT de Servicios Generales, Administrativos y Financieros, deberán informar inmediatamente al GIT de Apoyo Informático, las novedades de ingreso, retiro, vacaciones, incapacidades, etc. de los funcionarios que prestan sus servicios a la Entidad, a fin de actualizar el uso de los recursos tecnológicos que le son asignados, lo anterior de acuerdo con lo dispuesto en los procedimientos GTH-PRC17–Selección, vinculación y desvinculación del personal de planta y GAD-PRC21–Retiro de privilegios contratistas.

6. GESTIÓN DE CUENTAS LINUX

- Se prohíbe la creación de cuentas sin propósito definido o sin autorización previa.
- Cada usuario deberá contar con una cuenta individual, quedando prohibido el uso de cuentas compartidas.
- El nombre de usuario deberá seguir el estándar institucional (inicial del primer nombre + apellido. En caso de una cuenta existente se usará la primera letra del segundo apellido.
- Las cuentas deberán crearse bajo el principio de mínimo privilegio.
- Queda prohibido otorgar privilegios administrativos directamente al usuario final. A excepción de aquellos usuarios que dentro de sus actividades este la administración de un sistema de información (Ej. Aula Virtual)
- El acceso privilegiado deberá gestionarse mediante **sudo**, con reglas explícitas y auditables en el archivo /etc/sudoers.
- En el caso de una asignación a grupos deberá realizarse de acuerdo con funciones específicas del usuario.
- Las contraseñas deberán cumplir con:

-Complejidad adecuada (mayúsculas, minúsculas, números, símbolos).
-No reutilización de las últimas *5* contraseñas.
-Expiración según lo establecido por la guía de la Entidad de acuerdo con el numeral

5.4.3 Cambio de contraseña para usuarios

-Se deberá habilitar el bloqueo por intentos fallidos

- Las contraseñas temporales deberán ser cambiadas al primer inicio de sesión.
- Se prohíbe el acceso directo del usuario root mediante SSH.

- Se deben restringir los accesos SSH por usuario, grupo, red o dirección IP, según corresponda.
- Deberán registrarse todos los eventos de inicio y cierre de sesión.
- Las cuentas de funcionarios y contratistas con usuarios administradores y que no estén vinculados a la entidad deberán ser **bloqueadas de inmediato** o deshabilitadas.
- Todos los eventos de autenticación deberán ser registrados en archivos de log como:
  /var/log/auth.log
- El acceso root solo deberá utilizarse para tareas estrictamente necesarias.
  - La contraseña de root deberá estar custodiada bajo un mecanismo seguro (por ejemplo, bóveda de contraseñas) con acceso restringido.