CONTADURÍA GENERAL DE LA NACIÓN	**POLITICA DE ADMINISTRACION DE USUARIOS Y/O CONTRASEÑAS**		
	PROCESO:	**GESTIÓN TIC`S**	
	PROCEDIMIENTO:	**ADMINISTRACIÓN DE PLATAFORMA TECNOLOGICA**	
	FECHA DE APROBACION: 12/11/2020	**CODIGO: GTI02-POL01**	**VERSION: 05**

1. OBJETIVO:

Documentar los lineamientos de gestión de usuarios, perfiles y contraseñas.

2. ALCANCE:

La presente política será aplicada al control de acceso lógico a los siguientes componentes tecnológicos:

- Administración de Infraestructura (Servidores y Switches)
- Administración de Herramientas de Seguridad (Perimetral y Lógica)
- Plataformas de procesamiento (o sistemas operativos)
- Bases de datos
- Sistemas de información
- Servicios de red y comunicaciones (ej.: correo electrónico, Internet, impresoras, etc.)

3. RESPONSABLES DE CUMPLIMIENTO:

Son responsables del cumplimiento de este procedimiento todos los administradores de infraestructura, administradores de seguridad, funcionarios de la Contaduría General de la Nación y terceros que hagan uso de cualquier recurso informático perteneciente a la misma.

4. 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 un entorno (de red, plataforma o sistema).
- **Perfil**: conjunto de permisos o funciones que puede realizar un usuario. Los perfiles se asocian a las cuentas de usuario.
- **Administradores**: Se refiere tanto a los Administradores de Infraestructura (Servidores y Switches) como a los Administradores de Herramientas de Seguridad (Perimetral y Lógica).

5. ESTÁNDARES PARA LA CREACIÓN DE NOMBRES DE USUARIO PARA LAS ARQUITECTURAS UNIX:

Este nombre es asignado por el responsable del componente tecnológico, será la "identificación" del usuario y se ingresará al inicio de uso del componente tecnológico.

- **Pautas y Características:**

El ID del usuario tendrá una longitud mínima de 4 (cuatro) y una longitud máxima de 8 (ocho) caracteres.

Para la asignación de usuarios para acceso a un sistema, se tendrán en cuenta los siguientes criterios:

Los usuarios se clasificarían por tipos:

D - Usuarios de Desarrollo

S - Usuarios de Soporte

F - Usuarios Finales

T - Usuarios Temporales

El usuario será el mismo a través de todos los sistemas, ambientes y/o máquinas donde deba acceder.

Los usuarios se construyen independientes de los sistemas que acceden.

Los nombres de usuario siempre serán en minúsculas.

Los usuarios pertenecerán a un grupo de acuerdo a la dependencia en que trabajen, por ejemplo, Consolidación.

El acrónimo para nombrar usuarios sería:

- 1 carácter alfabético que determina el tipo de usuario
- 2 caracteres alfabéticos que describen la inicial del nombre y del primer apellido
- 3 caracteres numéricos para determinar un consecutivo, Iniciando en 001, que determina el número de usuario en el sistema.

Por lo tanto un usuario sería así:

d usuario de Desarrollo

lm primer carácter nombre de usuario (leonardo), segundo carácter inicial del primer apellido de usuario (martinez).

006 el orden de creación del usuario en el sistema

Usuario: dlm006

6. ESTÁNDARES PARA LA CREACIÓN DE NOMBRES DE USUARIO PARA LAS ARQUITECTURAS WINDOWS Y CORREO ELECTRÓNICO:

Como norma para todos los ID de usuario exceptuando los ID de Administradores de Seguridad y los ID de Administradores de Plataforma y de Sistemas Operativos Unix, AIX, Windows y Bases de Datos se utilizará la inicial del primer nombre y el primer apellido del usuario (Ej. Juan Fernando Pérez Campo será jperez)

Para los nombres y apellidos compuestos se tendrán en cuenta siempre el primer nombre y el primer apellido. Puede suceder que ya exista un usuario con la misma identidad, por lo que se utilizarán las iniciales del primer y segundo nombre y el primer apellido. Ejemplo: Si ya existe el usuario jperez se creará el usuario jfperez, así sucesivamente, en caso que el usuario no tenga segundo nombre se utilizará la inicial del segundo apellido, es decir jperezc.

7. CONTRASEÑAS

7.1. Parámetros Generales de las Contraseñas

a) Toda contraseña debe tener por lo menos una combinación de caracteres especiales, alfanuméricos y mayúscula. Se recomienda el uso adicional de caracteres especiales (,.;:><\+*/=(){}[]!¡¿?"#%|$&°~¬@Çç-_), no superior a 30 de ellos.

b) Se recomienda que toda contraseña tenga una longitud mínima de 8 caracteres y máximo de 15.

c) Evite utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)

d) No usar referencias comunes, como el nombre del servidor, del administrador u otros similares.

e) La contraseña actual no debe ser igual o parecida en su estructura (ej: p1: Juan01admin, p2: Juan02admin) a ninguna de las últimas 5 contraseñas utilizadas. Esto se debe garantizar por parte de los administradores a través del Sistema Operativo o por GPO's por parte del administrador de dominio.

f) No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos y recursos tecnológicos en documentos de texto dentro del ordenador)

g) Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso a máximo tres (3), como sucede en una tarjeta de crédito y cajeros, y que el usuario se bloquee si se excede el número de intentos fallidos permitidos. En este caso deberá abrir un ticket en la mesa de servicio para requerir el restablecimiento de la contraseña.

h) Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

i) No utilizar la característica de "Recordar Contraseña" existente en algunas aplicaciones y/o navegadores de internet (Firefox, Internet Explorer, Google Chrome)

7.2. Asignación de contraseña para Usuarios Generales

Para el ingreso de un usuario a los diferentes sistemas se debe crear la solicitud en Service Desk previo diligenciamiento del formato GTI010-FOR 01 - SOLICITUD DE CUENTAS DE USUARIO INSTITUCIONAL, el cual deberá ir adjunto a dicha solicitud.

Para el primer ingreso a los diferentes sistemas el responsable de la asignación de cada una de las cuentas de acceso a las aplicaciones o sistemas de información suministrará una contraseña temporal, para acceder a cada uno de los ambientes, el sistema le solicitará el cambio inmediato de contraseña.

7.3. Cambio de contraseña para usuarios generales

Cuando el usuario inicie la sesión con su ID (por Ej.: agarcia), aparecerá un mensaje indicando que su contraseña está próxima a caducar y debe cambiarse de acuerdo a los parámetros del numeral 6.1. Esta política esta implementada en el GPO para que se aplique cada 45 días.

7.4. Cambio de contraseña para administradores

El cambio de contraseña será necesario para usuarios con privilegios de administradores tales como:

7.4.1. Servidores bajo cualquier sistema operativo

7.4.2. Equipos activos de red (switch, enrutadores, etc)

7.4.3. Servidor de correo.

7.4.4. Servidores de aplicación (Was, IIS, etc)

7.4.5. Storage Manager

7.4.6. Sistemas de almacenamiento secundario

7.4.7. Servidores Web

7.4.8. Aplicativos de gestión o misión que posean el manejo de usuarios interno, independiente de usuarios del sistema operativo.

7.4.9. Servidor y consola de Antivirus

7.4.10. Servidor de alojamiento de la herramienta de monitoreo

7.4.11. Redes sociales

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 dos (2) veces en el año.

7.5.Almacenamiento

El registro de los cambios de clave se hará de forma manual con letra totalmente legible, en sobre debidamente etiquetado y sellado en original y copia, la primera reposará en las gavetas de almacenamiento de licencias y medios y la respectiva copia se entregará al coordinador del GIT de Apoyo Informático, quien la custodiará bajo llave.

La etiqueta en cada sobre debe identificar unívocamente los recursos de HW o SW cuya clave está en su interior.

En el interior del sobre deben definirse 3 items:

1. Recurso administrado

2. Login de usuario

3. Clave de

usuario Ej:

1. Recurso Administrado: SKYLAB
2. Login de usuario: root
3. clave de usuario: RsxdE3c54673

Lo concerniente a login y clave debe ser “case sensitive”, es decir, obligatoriamente se deben registrar en mayúsculas y/o minúsculas según sea el caso.

Nota: Cuando se presente un evento donde se deba realizar trabajo en casa y que impida el levantamiento y almacenamiento de las contraseñas de administración para la custodia, los usuarios administradores deberán mantener la última contraseña reportada, solo en caso que se presente algún evento que comprometa la disponibilidad, integridad y confidencialidad del componente se podrá cambiar, el administrador informará a las personas pertinentes la situación y se determinará procedimiento para intercambiar dicho sobre.

7.6.Confidencialidad

La contraseña es confidencial, de uso exclusivo del usuario, no podrá ser igual al nombre de usuario y no debe “**prestarse**” a otros usuarios. (Para más información consultar el Manual de seguridad de la información).

7.7. Administración de Contraseñas

7.7.1. Elección de contraseñas

Para el buen uso de las contraseñas se debe tener en cuenta los siguientes aspectos:

a) Las contraseñas no deben ser construidas con menos de ocho (8) caracteres.

b) No utilizar contraseñas que sean únicamente palabras (aunque sean extranjeras), o nombres (el de usuario, personajes de ficción, miembros de la familia, mascotas, ciudades, marcas, lugares u otro relacionado)

c) No utilizar contraseñas completamente numéricas con algún significado (teléfono, fechas).

d) Elegir una contraseña que mezcle caracteres especiales y alfanuméricos (mayúsculas minúsculas).

e) No usar palabras existentes en el diccionario, ni las mismas escritas en orden inverso.

7.7.2. Protección de contraseñas

a) No se debe permitir que individuos que no sean miembros de la Entidad obtengan acceso a los servicios de cómputo y comunicaciones de la Contaduría General de la Nación. Todos los servidores públicos y terceros (contratistas, proveedores de servicios y outsourcing) deben velar porque este tipo de situaciones no se presenten al interior de la Entidad.

b) Cada contraseña es de uso personal e intransferible. Los servidores públicos y terceros que trabajan para la Contaduría General de la Nación no han de revelar la contraseña de su cuenta a otros servidores públicos y/o terceros.

c) Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones por medio de la cuenta de otro funcionario.

d) Los servidores públicos y terceros que trabajan para la Contaduría General de la Nación deben notificar inmediatamente al GIT de Apoyo Informático si sospechan que alguien ha obtenido acceso sin autorización a su cuenta y debe modificarla en forma inmediata.

e) El usuario es responsable por la custodia de su contraseña. Debe evitar en lo posible digitar la contraseña mientras alguna persona está observando lo que escribe en el teclado. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su

contraseña.

f) Está prohibido enviar la contraseña por el correo electrónico, teniendo en cuenta que este no es un medio seguro, ni mencionarla en una conversación.

g) No se deben almacenar contraseñas en formato legible en archivos tipo “batch”, scripts de logon automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso o en otros sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.

h) Los servidores públicos y terceros que trabajan para la Contaduría General de la Nación deben utilizar contraseñas diferentes en cada uno de los sistemas a los cuales tengan acceso, solo se podrá utilizar contraseñas similares en diferentes sistemas cuando el GIT de Apoyo Informático haya informado directa y expresamente que esto no compromete la seguridad de la información de la Entidad.

i) Cuando se presente un evento donde se deba realizar trabajo en casa, el usuario debe crear un servicio al administrador del directorio activo a través de la mesa de servicio, para realizar el cambio de clave cuando ésta expire. Ya que un usuario no puede hacer cambios de contraseñas a través del escritorio remoto porque el servicio RDP no lo permite.

Observación:

Las solicitudes de cuentas de usuario para el Sistema CHIP se realizan a través de la apertura del servicio en Service desk y diligenciamiento del formato, con autorización previa del Subcontador de Centralización

8. BAJA DE UN USUARIO

8.1. Por Desvinculación

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 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** al GIT de Apoyo Informático, teniendo en cuenta los procedimientos GTH-PRC17 – Selección, vinculación y desvinculación del personal de planta, GAD-PRC21 – Retiro de privilegios contratistas, un listado actualizado del personal con 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