1. **OBJETIVO**

Facilitar a los Servidores públicos, contratistas y terceros de la Gobernación de Cundinamarca los lineamientos para la creación de contraseñas seguras para el acceso a los servicios, sistemas de información o sistemas informáticos de la Entidad, con el fin de reducir la posibilidad de acceso no autorizado y divulgación de la información.

1. **ALCANCE**

La presente guía aplica a todos los Servidores públicos, contratistas y terceros de la Gobernación de Cundinamarca que soliciten, autorización de acceso a aplicaciones y recursos necesarios para procesamiento de información de la entidad.

1. **TERMINOLOGÍA**

Los términos y definiciones aplicables para el registro de activos de información son los establecidos en la Norma NTC-ISO/IEC 27001, Modelo de seguridad y privacidad de la información – Mintic y la Guía.

* **Contraseña o clave:** Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto.
* **Administrador:** Es aquella cuenta de usuario que tiene todos los privilegios de manejar las aplicaciones de la entidad y puede controlar, administrar, acceder y modificar características que otros usuarios no pueden, así como instalar aplicaciones o modificar aspectos importantes de la configuración y elementos de la red o del domino.
* **Cuenta o tipo de usuario:** Clasificación del usuario para acceder o instalar aplicaciones en el equipo de cómputo, pueden ser local, administradora de red, estándar o invitado, entre otros.
* **Dominio:** El conjunto de [computadoras c](https://es.wikipedia.org/wiki/Computadora)onectadas en una [red informática q](https://es.wikipedia.org/wiki/Red_(inform%C3%A1tica))ue confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red.
* **Estándar:** Es aquella cuenta de usuario que tiene acceso a las funciones básicas del sistema operativo, herramientas y aplicaciones sin privilegios para hacer instalación controlar, administrar, acceder y modificar características. **Local:** Es aquella cuenta que por sus características tiene restricciones cuando el ordenador se encuentra unido al dominio.
* **Nombre de equipo:** Es el nombre asignado a un dispositivo conectado a una red informática.
* **Parche**: Es una actualización de cada una de las licencias utilizadas.
* **PC:** Equipo personal de cómputo.
* **Perfil:** Es un entorno personalizado de identificación por usuario.
* **Contraseñas cíclicas:** El usuario generara contraseñas compuestas por una combinación fija de caracteres y una combinación variable, pero no predecible. Un ejemplo de este tipo de contraseñas prohibidas es “Enero-2004”.
* **Tipo de equipo de cómputo:** Clasificación que se le asigna a los equipos de cómputo según su configuración y estilo así, Equipo de escritorio (Desktop), Portátil (Laptop), Todo en uno All In One (AIO), Estación de trabajo (WorkStation).
* **Usuario:** Es aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos.

1. **GENERALIDADES Y/O POLITICAS DE OPERACION**

* Las contraseñas son asignadas por parte de los Administradores funcionales de cada aplicación, para el ingreso a un servicio, sistema de información o equipo informático temporalmente, la cual deberá ser cambiada por parte del usuario, para que sea solo de su conocimiento.
* El administrador del sistema deberá utilizar contraseñas diferentes en las sesiones de usuario y como administrador.
* Es responsabilidad del administrador de cada sistema establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.
* Cuanto más segura sea la contraseña, más protegido estará el equipo o servicio de TI contra personal no autorizado y amenazas como hackers y software malintencionado. Siempre, se deben tener contraseñas seguras para el uso de servicios, sistemas de información o equipos informáticos.
* Para solicitar un servicio de soporte se debe realizar a través de correo electrónico a la mesa de ayuda bajo la metodología establecida en el procedimiento Gestión de requerimientos e incidentes de Servicio (Mesa de Ayuda) TIC A-GT-PR-007 el cual genera un ticket de atención.
* La solicitud de un nuevo acceso a un sistema se realizará por parte del supervisor del contratista o del jefe inmediato del funcionario al administrador funcional del sistema que requiera acceso, la solicitud se debe realizar a través de la mesa de ayuda TIC dando cumplimiento en lo establecido en el procedimiento Gestión de requerimientos e incidentes de Servicio (Mesa de Ayuda) TIC con código A-GT-PR-007, donde se generará un ticket de atención.
* El vencimiento de la contraseña esta parametrizada a la fecha de terminación del contrato o la desvinculación del funcionario.

1. **DOCUMENTOS APLICABLES**

A continuación, se enuncia los documentos que aportaron para la construcción de esta Guía:

* Política de Control de Acceso, código: A-GSI-POL-004
* Procedimiento Gestión de requerimientos e incidentes de Servicio (Mesa de Ayuda) TIC, código: A-GT-PR-007

1. **DESARROLLO**
   1. **Características de una contraseña segura**

Los servidores públicos, contratistas y terceros de la Gobernación de Cundinamarca son los responsables de establecer una contraseña segura, que cumpla con las siguientes características:

* La longitud de la contraseña deberá ser mínimo de 8 caracteres.
* Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
* Debe ser significativamente diferente de otras contraseñas anteriores.
* La contraseña deberá estar compuesta por combinación de los siguientes caracteres: Mínimo una letra Mayúscula, ejemplo: A, M, O, F, H, E, X, O; Mínimo una letra Minúscula, ejemplo: p, c, r, s, a, d, i; Mínimo un número (digito), ejemplo: 0, 1 ,2 3,4 5,6 7,8, 9; Mínimo un signo o carácter, símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios, por ejemplo: ! @ # $ % ^ & \* ( ) \_ - + = { } [ ] \ | : ; " ' < > , . ? / Exceptuando, los sistemas de información externos que no contemple caracteres especiales.
  1. **Qué no debe contener una contraseña**

A continuación, se relacionan algunos aspectos que no debe contener una contraseña:

* El nombre de usuario, el nombre de la Entidad o partes del nombre de la Entidad.
* Estar compuesta solo con una palabra completa, nombre común o números
* Nunca se debe utilizar, letras consecutivas, ya sea por orden alfabético o por secuencia en el teclado del computador, o palabras comunes, o sólo números o secuencia de éstos.
  1. **¿Cada cuánto debo cambiar la contraseña?**
* Cuando ha sido visualizada por una o más personas.
* Para usuarios nuevos, las contraseñas asignadas deberán cambiarse obligatoriamente en el primer inicio de sesión, para garantizar que solo el usuario conozca la contraseña después de creados los accesos tecnológicos.

1. **Responsabilidades del usuario**

Cualquier persona que tenga acceso o utilice la información de autenticación, debe asegurar que:

1. La información de autenticación secreta, como las contraseñas, se mantenga con carácter confidencial. La información de autenticación secreta personal no debe compartirse. La información de autenticación secreta utilizada en el contexto de identidades vinculadas a varios usuarios o vinculadas a entidades no personales, se compartirá únicamente con personas autorizadas por el administrador funcional.

b) La información de autenticación afectada o comprometida se cambiará inmediatamente tras la notificación o cualquier otra indicación de un compromiso que afecte la autenticación de esta.

c) Dado que el usuario y la contraseña son intransferibles en la Gobernación de Cundinamarca el funcionario o contratista es responsable de todas y cada una de las transacciones que se realicen en los sistemas con los usuarios que le hayan sido asignados