# POLITICAS DE SEGURIDAD DE LA INFORMACION

# CONTRALORIA DEPARTAMENTAL DEL TOLIMA

# GESTION TIC

## 1 Cambio periódico de contraseña para correos y aplicativos:

- Se debe realizar el cambio de contraseña, por lo menos cada 30 días, como medida preventiva de seguridad informática y como buena práctica para garantizar la confidencialidad e integridad de su información.

- El cambio de contraseña solo se debe hacer usando los medios institucionales; para este caso la interfaz del correo electrónico de la contraloría y desde equipos conectados a través de la red de Internet disponible en la entidad.

- La contraseña es personal e intransferible y es responsabilidad de cada usuario el buen uso que se le dé a los servicios de Internet institucionales.

- Mantener de forma segura todo tipo de contraseña que se emplee para ingresar a sistemas de información, para lo cual, no se debe escribir la contraseña en ningún lugar a donde terceros puedan tener acceso.

- Las contraseñas se deben conformar por combinación de Letras mayúsculas y minúsculas, números y caracteres especiales, para así evitar herramientas de generación de contraseñas. No se deben emplear palabras que se relacionen ni con la vida personal, ni familiar, ni laboral del funcionario. Se recomienda emplear contraseñas con longitud mayor a 6 caracteres, aunque idealmente lo mínimo debería ser de 8.

## 2 Políticas aplicables a los correos electrónicos:

Se tendrá en cuenta todo lo establecido para los correos electrónicos en el documento "**ESPECIFICACIONES USO DEL CORREO, INTERNET Y RED INSTITUCIONAL**" código EGT-01.

## 3 Políticas aplicables a uso de computadoras, correos electrónicos y aplicaciones:

- No ingresar a sus cuentas en lugares desconocidos o de poca confianza (como un café Internet o un equipo ajeno); algunas computadoras de uso externo podrían tener instalado algún programa que rastree las pulsaciones de teclas y podrían apropiarse de las contraseñas.

- Cerrar siempre las sesiones de correos electrónicos y aplicaciones cuando quede sola la computadora, así sea en breves periodos de tiempo

- Nunca se deben dejar almacenadas en la computadora las contraseñas de los correos electrónicos o aplicativos, es decir, no se debe usar la opción de "Recordar contraseña" que ofrece el navegador de Internet.

- Las computadoras deben estar protegidas por contraseñas de inicio de sesión, así mismo, deben tener activado el protector de pantalla, con contraseña, el cual debe ser activado cada vez que el funcionario deba ausentarse de forma temporal y, por ende, la computadora vaya a quedar sola.

- Diariamente y cada vez que se inserte un dispositivo USB, se debe ejecutar el antivirus que se encuentra instalado oficialmente en las computadoras de la entidad, analizando por completo el contenido de la computadora (todas las unidades).

- Cada vez que se inserte un dispositivo USB, se debe ejecutar el antivirus que se encuentra instalado oficialmente en las computadoras de la entidad, analizando por completo el contenido del dispositivo insertado.

## 4 Políticas para el uso y acceso a la Internet:

- Ningún funcionario debe conectarse, sin autorización de Gestión TIC, a la red WiFi de la entidad en sus computadoras personales y/o dispositivos móviles.

- Por ningún motivo se hará uso de las contraseñas de la red de Internet ni se suministrará tal contraseña a terceros, sin autorización de Gestión TIC.

También, se tendrá en cuenta todo lo establecido para el Internet, computadores, móviles y WiFi en el documento "**ESPECIFICACIONES USO DEL CORREO, INTERNET Y RED INSTITUCIONAL**" código EGT-01.

## 5 Políticas sobre los activos de información digitales:

Los activos de información digitales, para el caso de estas políticas, corresponde a todo tipo de archivo en formato digital, independientemente del medio empleado para su conservación o almacenamiento.

- Toda información en medios extraíbles, debe estar codificada (encriptada) y/o contar con contraseñas tanto para abrir como para modificar el documento, atendiendo a lo ya indicado en estas políticas sobre la conformación de las contraseñas.

- Se debe mantener en lugar seguro todo dispositivo que almacene información sobre temas relacionados con el quehacer diario en la entidad, evitando así que terceros puedan llegar a tener acceso a tal información.

- Es responsabilidad de cada funcionario realizar copias diarias de los archivos que han sido generados o que se han modificado, para lo cual, tal información debe descargarla en una memoria USB.

  No se deben emplear los medios extraíbles para el trabajo permanente con ficheros sino exclusivamente para mantener copias de los mismos.

- Mientras el sistema de copias de seguridad en red no se encuentre configurado para backups automáticos de los archivos que cambian diariamente, cada funcionario debe realizar sus propias copias de seguridad, en el sistema en red, al menos una (1) vez por mes, entre el 25 y 30 de cada mes.

  Esto será aplicable una vez el sistema de copias de seguridad en red se encuentre totalmente implementado y se hayan realizado las respectivas capacitaciones.

- El personal de Gestión TIC, realizará copia de seguridad del contenido del sistema de copias de seguridad en red, los primeros diez (10) días de cada mes. (Condicionado a la total implementación y capacitación sobre el sistema de copias de seguridad en red).