# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

**Versión 01**

**Gestión de TIC´s**

**Santiago de Cali, agosto 2022**

# CONTENIDO

# 1. INTRODUCCIÓN

La información institucional se reconoce como un activo valioso y en la medida que los sistemas de información apoyen a los procesos misionales, se requieren estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Nuestra institución, los sistemas y la red de información enfrentan amenazas de seguridad que incluyen, entre otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación, Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Con la promulgación de la presente Política de Seguridad de la Información el Instituto Popular de Cultura formaliza su compromiso con el proceso de gestión de TIC’s para garantizar la integridad, confidencialidad y disponibilidad de la información.

Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos” las cuales deben ser adoptadas por todos los funcionarios, contratistas, proveedores y todo personal que utilice los servicios de tecnologías de la información que ofrece el Instituto.

## 2. ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características:

- Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.
- Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- Posibilidad de Auditoría: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- Protección a la duplicación: Los activos de información son objeto de clasificación y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- Legalidad: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.

## 3. OBJETIVO

El objetivo del presente documento es establecer la política en seguridad de la información del Instituto Popular de Cultura, con el fin de establecer lineamientos que regulen la gestión de la seguridad de la información, asegurando el cumplimiento de

los principios de confidencialidad, integridad, disponibilidad, salvaguarda, legalidad y confiabilidad de la información.

## 4. ALCANCE

La presente política se elabora en cumplimiento de las disposiciones legales vigentes, con el objetivo de gestionar adecuadamente la seguridad de la información, los sistemas y servicios tecnológicos que preste el Instituto Popular de Cultura IPC, es de aplicación para toda la comunidad, ya sean visitantes, contratistas, funcionarios, proveedores, docentes y comunidad estudiantil, sin importar su nivel jerárquico.

Toda vulnerabilidad que se detecte será responsabilidad del usuario y dependiendo de la gravedad se aplicarán las sanciones que sean convenientes.

## 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La información es el principal activo de una organización, en la red cada día se generan nuevas alertas que pueden afectar de manera inminente un sistema, provocando fallas irreparables, para lo cual las organizaciones deben implementar mecanismos para salvaguardad los datos que se consideren vulnerables y que se pueden perder ya sea por virus o personas mal intencionadas. Perder información de manera parcial o total, genera un gran traumatismo y más si no se tiene respaldo de la misma.

El instituto popular de cultura a través de la oficina de TIC's se compromete a proteger la información institucional que se genera, circula, procesa y almacena por medios digitales.

La oficina de TIC's liderará la revisión, cumplimiento y mejoramiento continuo de la seguridad informática y generará la documentación necesaria como procedimientos, manuales, instructivos y demás elementos que sean necesarios para tal fin.

En el Instituto Popular de Cultura, las políticas relacionadas a la Seguridad de la Información como son el presente documento, la Política de seguridad física y la Política de tratamiento de datos personales deberán ser difundidas a todo el personal involucrado en su definición.

Toda decisión avalada por la Dirección del Instituto deberá ser cumplida a cabalidad por el personal que realice actividades en la misma.

## 5.1. Políticas Generales

Los funcionarios se deben regir por los siguientes lineamientos:

1. Los usuarios se regirán por los lineamientos técnicos establecidos por el área de las TIC's.
2. Todo funcionario es responsable de reportar inmediatamente las anormalidades e incidentes de seguridad que observe en los sistemas, tanto a su superior como al área de las TIC's.
3. Las modificaciones y/o divulgación de los datos e información de los sistemas deben estar estrictamente restringidas a las transacciones y procesos expresamente diseñados para tal fin.

4. El área TIC's tendrá como responsabilidad la administración de cada red LAN en las diferentes sedes de la institución, además de dar el apoyo en el mantenimiento preventivo y correctivo de los equipos de cómputo en cada sede.

5. Todo el equipo Informático (computadoras, estaciones de trabajo, estaciones gráficas, servidores, dispositivos móviles), que esté o sea conectado a la red de la institución, debe sujetarse a las normas y parámetros de instalación y configuración de red que sean implementados y normalizaos por el área de las TIC's y la Dirección.
6. El encargado del almacén, junto a la oficina de las TIC's deberá tener un registro de todos los equipos en propiedad de la institución y deberá ingresar en el sistema de inventarios todo equipo que este en uso por el IPC, el cual deberá contener el nombre del funcionario que tiene a cargo el equipo o recurso tecnológico y mantener el inventario fiscal debidamente actualizado.
7. El personal (nombrado o contratista) que tenga como finalidad de su contrato la prestación de servicios y/o administración de plataforma tecnológica, soporte técnico, redes de comunicaciones o responsabilidades relacionadas con el funcionamiento y administración de la red de datos de la entidad, estará bajo órdenes, supervisión y mando del Profesional responsable del área de las TIC's.
8. El área de TIC´s es la única facultada para administrar y configurar el acceso a los recursos de las plataformas tecnológicas en el Instituto de acuerdo a la descripción de cargo.
9. Todo aquel elemento o equipo de hardware retirado en forma de préstamo de las instalaciones de la entidad debe tener su respectiva orden de salida con la firma de quien retira y del líder de proceso y la aprobación del área de TIC´s.

10. Todo aquel elemento o equipo de hardware de propiedad de la Institución que sea reintegrado o devuelto debe ser revisado por el área de TIC´s.
11. El manejo de la información y los servicios en la nube propios de la institución están autorizados siempre y cuando se cumpla con los acuerdos de confidencialidad.
12. El personal que extraigan través de diferentes medios removibles datos que corresponda a información interna de propiedad del instituto, debe garantizar los acuerdos de confidencialidad.
13. Está estrictamente prohibido la divulgación, cambio, retiro o pérdida no autorizada de información del Instituto almacenada en medios físicos removibles, como USB, Disco, entre otros.
14. El área de TIC´s en equipo con el área encargada del Almacén, dando cumplimiento al procedimiento de baja de equipos y con la previa autorización del comité de bajas, deben retirar y dar de baja aquellos equipos (servidores, desktop o portátiles) que, por sus características técnicas, software base, soporte han cumplido su vida útil y son punto vulnerable de seguridad.
15. Es responsabilidad de los funcionarios el garantizar recoger las impresiones al momento de generarlas, no se deben dejar por largo periodo de tiempo en la impresora.
16. Cuando un usuario termina contrato y no lo renueva, el área de TIC´s es la responsable de suspender las cuentas de correo electrónico y el acceso a los diferentes sistemas, por lo cual se debe tener en cuenta los siguientes puntos:
    a. El Líder de cada área y el área Jurídica debe notificar al área de TIC´s cuáles son los funcionarios que no continuarán en contratación, esta notificación se debe realizar previamente al retiro del funcionario.

b. El área de TIC's debe proceder a bloquear el acceso de ingreso a todos los sistemas de información.
c. El área de TIC´s debe proceder a realizar copia de seguridad de la información en los diferentes sistemas y almacenarla en el servidor de Backups.

## 5.2. Política de Control de Acceso

La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática.

El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.

1. Los equipos de cómputo como primer nivel de seguridad, deben ser configurados con dos roles de inicio de sesión, el rol administrador y el rol secundario que tendrá permisos limitados.
2. Cada usuario debe tener una credencial de inicio de sesión (Usuario y Clave) única e intransferible dentro del sistema de control de accesos.
3. Las claves de acceso a los equipos tecnológicos son personales e intransferibles y solamente deben ser utilizadas por el funcionario para el acceso al mismo. Está totalmente prohibido que un funcionario autorice a un tercero para que utilice sus credenciales de acceso al sistema, será responsable de las actividades y transacciones que sean realizadas bajo sus credenciales.
4. Ningún funcionario deberá acceder a los equipos de cómputo, a los sistemas de información, a la red o a los servicios TIC, utilizando una cuenta de usuario o clave de otro usuario.

5. Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que registró o se le asignó la clave.
6. Los funcionarios no podrán realizar instalaciones de programas sin ser autorizados por el área de las TIC's, toda falla que se pueda generar por vulnerar este punto será responsabilidad del funcionario y deberá subsanar el incidente generado.
7. Los funcionarios deben seguir los siguientes parámetros para la creación de las claves de acceso a los equipos de cómputo y sistemas de información:
   a. La clave de usuario debe ser alfanumérica, contener caracteres especiales y una longitud no menor a 8 (ocho) dígitos sin utilizar espacios en blanco.
   b. Deben incluir caracteres alfanuméricos (al menos un digito (1) de este tipo).
   c. La clave de acceso no debe ser el nombre, ya que sería un dato descifrable y se puede generar una vulnerabilidad.
   a. No se debe repetir claves de acceso al sistema, utilizadas con anterioridad.
   b. El nombre de usuario debe ser diferente con la clave de acceso.
   c. No se deben utilizar claves con fechas de nacimiento, nombres de familiares, números de identificación.
   d. Las claves de acceso se deben cambiar mínimo 2 (dos) veces al año.
8. Se debe revisar por parte del área de TIC's los derechos de acceso (usuarios configurados) en todas las terminales activas en la Institución (equipos de cómputo, tablets) periódicamente con un mínimo de interacciones de 2 (dos) veces al año, verificando que los accesos sean los asignados en configuración inicial. Si estos no corresponden, se deben deshabilitar y realizar un acta de los hechos ocurridos.
9. Es responsabilidad del funcionario una vez terminada su jornada laboral apagar el equipo de cómputo.

10. Tendrá acceso a las diferentes terminales de trabajo solo el personal del área de las TICs, que posee las credenciales de acceso al usuario master o administrador.
11. El funcionario debe garantizar el no anotar y/o almacenar en lugares visibles las credenciales (usuario y/o claves) de acceso a los sistemas.
12. El área de TIC´s debe realizar copias de seguridad a las diferentes terminales de trabajo como mínimo 2 veces al año o en intervalos de duración del contrato laboral celebrado entre el funcionario y la entidad. Las copias de seguridad se extraerán en un disco duro portable y se pasara la información al servidor de datos.
13. El área de TIC´s debe realizar mantenimiento, preventivo y/o correctivo 2 (veces) al año, o en tiempo por fuera de este límite si en los equipos (terminales de trabajo) se presenta alguna falla.
14. Todo equipo que sea ingresado a la institución debe ser registrado en la portería principal, diligenciando la marca del equipo, serial, hora de ingreso, nombre completo y firma de quien ingresa el equipo.
15. Si un tercero desea utilizar un dispositivo de almacenamiento en los equipos, este debe ser examinado por el área de TIC’s con el fin de descartar la presencia de virus.
16. Los funcionarios deben bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.

## 5.3. Política de Conectividad (Internet)

El acceso a Internet e Intranet, es una herramienta de trabajo que provee la Institución a sus funcionarios, por lo tanto, es responsabilidad de cada usuario, utilizar prudente y apropiadamente este servicio.

1. Todo evento que se dé a través del uso de este servicio, será administrado, monitoreado y regulado por el área de TIC's el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad e integridad de la información.
2. Todo evento que se dé a través del uso de este servicio, será administrado, monitoreado y regulado por el área de TIC's el cual tendrá la potestad de realizar las acciones pertinentes en pro de proteger, asegurar y garantizar la disponibilidad de los equipos informáticos (computadores, servidores y equipos de telecomunicaciones) para dar continuidad al servicio de internet.
3. Los usuarios de la red de internet tienen prohibido el acceso a sitios de Internet que no tengan relación alguna con los objetivos institucionales, tales como los relacionados con: sexo, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas y uso de la red.
4. Toda información que sea descargada de internet debe tener relación con los objetos misionales, gerenciales o de apoyo a la institución y las diferentes funciones que lleva a cabo el funcionario.
5. El área de TIC´s debe garantizar la instalación de un Antivirus en todas las terminales de cómputo y es responsabilidad del funcionario mantener activo el antivirus, con el fin de minimizar los riesgos sobre descarga de archivos realizados desde la web que afecten tanto al hardware, software e información.

6. Si se genera en el navegador alguna alerta, mensaje, ventana emergente o algún evento que genere sospecha de virus o de ataque, es responsabilidad del funcionario informar al área de TIC's para verificar la procedencia del mismo y controlar el riesgo.
7. Las actualizaciones de sistema operativo y de software solo son realizadas por el área TIC's, no está permitido la instalación de actualizaciones sin antes verificar su procedencia.
8. El acceso remoto a los equipos de cómputo y equipos de telecomunicaciones solo está permitido y podrá realizarlo área de TIC´s. y en caso esporádico que por algún motivo el área financiera y Dirección requieran conexión remota deberán solicitarlo por escrito y bajo previa autorización de la Dirección el área de TIC´s concederá el acceso.
9. El área de TIC´s será responsable de renovar las claves de acceso a la red inalámbrica con una frecuencia de 2 veces al año.
10. El área de TIC´s debe garantizar que los equipos de cómputo y tabletas asignados a la Biblioteca se utilicen como equipos de consulta con restricciones a paginas tales como las relacionadas con: sexo, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas y uso de la red.

### 5.3.1. Política de Redes Inalámbricas

Esta política establece las reglas para el uso de tecnología inalámbrica. La administración de los recursos de tecnologías de la información y las comunicaciones es importante para el cumplimiento y desarrollo de las labores, las redes inalámbricas requieren de un alto grado de responsabilidad por parte de los

usuarios de la red para aprovechar y maximizar los beneficios de la tecnología, brindando cobertura de red inalámbrica y un sistema de comunicaciones seguro en las edificaciones de la entidad.

Toda persona que utilice la red inalámbrica de la institución debe dar un uso apropiado a la misma.

1. Los quipos inalámbricos deben ser instalados por el personal de TIC's de la institución, estos deberán ser monitoreados con el fin de garantizar su buen uso.
2. Los usuarios deben evitar realizar un mal uso de la red inalámbrica de la institución, como el acceso a páginas o aplicaciones que contengan sexo, racismo, apuestas, actividades criminales, drogas, juegos y cualquier otra que se estime conveniente restringir que puedan afectar el desempeño de la red inalámbrica.
3. Para usuarios visitantes en la sede de San Fernando el área de TIC´s es el responsable de restringe la conexión a carpetas compartidas y solo se habilitará a los visitantes la red llamada "Cafetería" con el fin de minimizar los riesgos en cuanto acceso a información interna que fluye en la red.

## 5.4. Política de Correo Electrónico

El correo electrónico, es una herramienta de trabajo que la Institución provee a sus funcionarios, por lo tanto, es responsabilidad de cada usuario, utilizar prudente, responsable y apropiadamente este servicio.

1. Todo evento que se dé a través del uso del correo electrónico, será administrado, monitoreado y regulado por el área de TIC's el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad,

confidencialidad e integridad de la información de la institución, así mismo, reportará a la Dirección cualquier uso indebido del servicio.

2. Es responsabilidad de los funcionarios que el contenido de los mensajes creados, enviados, recibidos y almacenados se limiten a los propósitos misionales y/o operativos del Instituto, su contenido debe ser respetuoso y no debe atentar contra la imagen ni integridad moral de sus funcionarios y usuarios.
3. Queda totalmente prohibido enviar mensajes de correo electrónico masivos por parte de personal no autorizado, tales permisos quedan reservados para Dirección, Coordinadores, o áreas de comunicaciones internas de la entidad y bajo supervisión del área de TIC´s.
4. Las cuentas de correo electrónico institucional deberán ser usadas solamente para fines laborales, no para suscripción de servicios y/o listas de correo relacionadas con temas personales.
5. El tamaño de los archivos que circulan por correo electrónico o a través de los canales de comunicación, así como el espacio del buzón asignado a cada usuario para el almacenamiento de estos archivos, tendrá un límite de 15 Gb tanto en mensajería como en Drive, así mismo cada usuario está obligado a iniciar sesión y revisar periódicamente su cuenta de correo institucional.
6. La información considerada por cada área como sensible debe evitarse compartir por medio de correo electrónico, pero en caso de ser necesario el funcionario debe comprimir y cifrar la extracción de archivos, asegurar que sea destinada exclusivamente a personal autorizado y el funcionario será el directamente responsable de la integridad y confidencialidad de dicha información.
7. Para el almacenamiento en la nube, los funcionarios deberán utilizar la herramienta dispuesta por la institución para tal servicio, en este caso será

Google Drive, esta prohibido que los funcionarios almacenen información en correo distintos a los terminados en correoipc.edu.co, si el área de TIC´s sorprende a un funcionario realizando esta actividad en correos no institucionales se realizará el reporte tanto al supervisor como a la Dirección.

8. Es responsabilidad de los Usuarios que tener en cuenta que los mensajes creados, recibidos o almacenados en la bandeja principal de la cuenta de correo, no deben ser impresos, especialmente los que están configurados como reservados o confidenciales; Se debe minimizar las impresiones de documentos y solo imprimir los que realmente se considere como necesario.
9. La institución cuenta con las herramientas blindadas por google para la protección de los servicios de los correos electrónicos y el uso del antivirus licenciado, sin embargo los funcionarios no deben abrir mensajes desconocidos o que desconozcan su propósito, ejemplo: “mensajes de foto multas ya que la institución no cuenta con vehículos propios, ganador de premios en los cuales no ha participado, mensajes de la DIAN, correos no institucionales, entre otros”; en caso de recibir un mensaje de dudosa procedencia, es obligación del funcionario comunicarlo al área de TIC’s de la institución antes de dar trámite al mismo.
10. En caso de olvido o pérdida del acceso al correo institucional, el funcionario debe solicitar al área de las TIC’s el restablecimiento de la misma.
11. El área de TIC´s solo creará y habilitará cuentas de correo electrónico a Usuarios que el supervisor o la dirección avalen por escrito.
12. Ningún usuario deberá permitir a otro enviar correos utilizando su cuenta.

## 5.5. Política de Sistemas de Información

La instalación, diseño, creación y uso de los sistemas de información se rigen por las solicitudes, viabilidades y objetivos específicos en pro del desarrollo de la institución.

1. En todos los desarrollos de sistemas de información se debe considerar como obligatorio la seguridad desde el inicio del ciclo de vida del software hasta su fin. Cada desarrollo debe contener los logs de las pruebas realizadas antes de ser desplegados en producción. Se deben prever todos los riesgos y posibles complicaciones que surjan para su desarrollo y puesta en marcha.
2. Durante las fases de desarrollo, mantenimiento y ajustes, se deben tener todos los protocolos de seguridad activos tales como:
   a. Copias de seguridad (código y bases de datos).
   b. Migración de datos (para desarrollos nuevos).
3. Para desarrollos nuevos, se debe disponer de una persona idónea que pueda servir de supervisor, guía y se deben llevar controles sobre los avances y los alcances planteados previamente.
4. Todo nuevo desarrollo debe tener entre sus líneas de código comentarios sobre la función, con el fin de tener aclaratorias sobre cada bloque de código y facilitar la comprensión y el análisis sobre su propósito.
5. En el análisis y clasificación del riesgo del sistema y en la fase de diseño, se deberá definir los requerimientos de seguridad, desde la vista del administrador como del usuario final que manipulara el sistema, las medidas de seguridad deberán quedar plasmadas en un documento con el fin de ser establecidas.

6. El área de TIC´s deberá documentar todos riesgos previstos durante desarrollos, ajustes, actualizaciones y notificar tanto al interventor como a Dirección y solo se ejecutarán bajo previa autorización.
7. Las pruebas de desarrollo deben ser documentas, para ser aprobadas por el interventor y por el usuario final.
8. La calidad del software ya sea en desarrollo o mantenimiento debe cumplir con estándares de calidad para garantizar la confiablidad del sistema.
9. El proceso de puesta en producción de las aplicaciones, de los sistemas o de sus actualizaciones, debe realizarse de tal forma que no deteriore los servicios a los usuarios o la operación normal, por tanto, el área de TIC´s debe coordinar adecuadamente y realizar cronogramas y horarios preestablecidos para dicha actividad.
10. El área de TIC,s debe realizar copias antes, durante y después de cada desarrollo o mantenimiento con el fin de tenerlas como contingencia.
11. La empresa contratada (Servidor Contable, Plataforma Académica, Sitio Web y Sitio de Biblioteca) será responsable de mantener la operatividad del servidor y atenderá las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware e información almacenada en el sitio.
12. Para los servicios instalados en local, el área de TIC's será responsable de monitorear la utilización de los recursos de hardware en el servidor, esto con el fin de proceder a la actualización del mismo en el caso de ser requerido para garantizar la continuidad de los servicios.
13. Para los servicios de mantenimiento, migración o nuevos desarrollos, el área de TIC´s debe notificar a los usuarios las ventanas de mantenimiento o la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad del mismo.

14. El área de TIC´s debe documentar todo cambio o ajuste al sistema y deberá contar con una ventana de mantenimiento la cual debe indicar fecha, responsable, servidor y aplicativo afectado, además del motivo de los cambios efectuados.

### 5.5.1. Política de Separación de Ambientes

La entidad deberá contar con ambientes separados para desarrollo, pruebas y puesta en producción de los Sistemas de Información, bajo ningún motivo se podrá desarrollar aplicaciones en el ambiente productivo.

1. Las funciones de desarrollo de aplicaciones, pruebas funcionales y aceptación, deben estar separadas y ser realizadas por funcionarios distintos, a efecto de asegurar una adecuada segregación de funciones y calidad en la entrega del producto conforme a la necesidad del usuario final.
2. Cuando se realizan las pruebas del nuevo Sistema de Información debe realizarse previamente en un ambiente de pruebas del sistema, preferiblemente virtualizado, con el fin de no comprometer la información ni las bases de datos de la institución o de los funcionarios.
3. Toda prueba realizada en el software (desarrollo o mantenimiento) se debe realizar en un ambiente de pruebas local antes de pasarlo al ambiente de producción, se deben considerar las vulnerabilidades con el fin de minimizar y detectar los errores.
4. Toda prueba debe realizarse utilizando como base el documento de mapa de pruebas el cual contiene todos los casos de pruebas a realizar que garantiza el cumplimiento de los requerimientos de desarrollo solicitados por el usuario.

## 5.6. Política de Transferencia de Archivos

La documentación software o cualquier tipo de información de uso, no debe ser transferida a terceros sin que exista autorización superior o un compromiso de confidencialidad entre el instituto popular de cultura y terceros.

1. Toda información que se genere, procese, almacene y/o transite por la red se considera propiedad del Instituto Popular de Cultura.
2. La información transmitida, procesada producto de las funciones del personal y que concierne al Instituto Popular de Cultura o a sus usuarios, no podrá ser interceptada o divulgada bajo ninguna circunstancia, por ningún usuario interno que tenga acceso a la red.
3. Queda totalmente prohibido cargar información de la entidad a nubes públicas como los son Dropbox y OneDrive, en caso de requerirse la transferencia de información entre Sedes o hacia un externo, se deberá usar el servicio de nube (Google Drive), en donde se podrá:
   a. Dar permisos de acceso, consulta y/o modificación por correo electrónico.
   b. Asignar tiempo de publicación de la información.
   c. Para personas externas solo se les puede dar permisos de lectura y si se requiere bajo previa autorización del líder del área se podrá dar permisos adicionales.

## 5.7. Política de Copias de Seguridad

El área TIC'S, ha asignado a cada perfil de usuario de dominio una unidad en la cual almacenaran información de carácter estrictamente laboral, no se podrá almacenar fotos, música, videos e información personal.

La institución tiene una carpeta creada en red para compartir información (Kapitan), en esta carpeta podrá compartir información relacionada con sus labores, cada usuario deberá extraer la información que se encuentre ahí almacenada y guardarla en su disco local.

Cada trimestre del año el área de las TIC's eliminará la información que se encuentra en esta carpeta, esto con el fin de liberar espacio en el servidor y minimizar los riesgos con la información ahí almacenada.

1. Al finalizar el contrato de cada funcionario, este será responsable de solicitar la realización de la copia de seguridad de su equipo, además de solicitar la firma del respectivo paz y salvo por parte del área de las TIC's.
   Nota: no se firmará el documento de paz y salvo sin antes haber realizado la copia de seguridad.
2. Es obligación de todos los funcionarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse, dicha copia deberá ser periódica e incremental, debe ser almacena en el disco local D, A o B; el funcionario deberá comunicarse con el área de TIC'S con el fin de establecer los medios adecuados para conservar tales copias de seguridad.
3. El área de TIC´s realizará copias de seguridad con una frecuencia de 2 veces al año, se realizará un análisis de la misma, información que no corresponda con las labores de los funcionarios, tales como imágenes personales, música entre otras serán eliminadas.
4. El área de TIC´s realizará pasará las copias de seguridad al servidor de respaldo y se mantendrá una copia por un periodo de 6 meses en los discos portables para su consulta.

5. El área de TIC´s pasará las copias de seguridad al servidor de respaldo utilizando el método de conservación del archivo más actual.
6. El área de TIC´ habilitará el acceso solo en los momentos necesarios y que tengan una previa solicitud por escrito (físico o email). Los archivos visualizados por los funcionarios solo serán de lectura, no podrán borrar o agregar información adicional, el servidor se desactivará de la red al terminar la consulta por parte de los funcionarios.

## 5.8. Política de Software y Licencias

En los equipos de cómputo solo se debe tener instalado el software debidamente licenciado y autorizado por el área de las TIC's.

1. Todo software instalado en los equipos debe tener la licencia para su uso, dejando de lado al software de licencia libre que solo serán instalados por el área de TIC's.
2. El área de TIC´s deberá llevará una hoja de vida de los equipos de cómputo con el software instalados, licencias y tiempo de vida de las mismas.
3. Todo software libre o de licencia abierta que se requiera instalar en los equipos, se deberá realizar solicitud previa al área de TIC's para realizar pruebas sobre el mismo antes de realizar una instalación individual o masiva.
4. Todas las estaciones de trabajo deben tener instalado un antivirus ya sea el que viene por defecto en el sistema operativo Windows o el contratado por la institución, la base de datos de los mismos se debe actualizar automáticamente y una vez por semana.

5. El software instalado y sus recursos son de uso exclusivo para las actividades relacionadas con las actividades que realiza cada funcionario.

## 5.9. Conservación de Recursos

El mantenimiento preventivo se realizará en periodos de 6 meses mediante actualizaciones, copias de seguridad y limpieza del equipo.

1. El mantenimiento correctivo se realizará en los tiempos en que los funcionarios reporten la falla, se deberá realizar copia de seguridad o rescate de la misma y luego definir si es necesario reinstalar los programas necesarios.
2. El cambio de piezas o repotencialización de los mismos solo se realizará si se tienen las piezas necesarias.
3. Se prohíbe a los funcionarios eliminar virus informativos de los sistemas, cuando estos estén infectados ya que pueden producir más daños en la información o programas.
4. Está prohibido descargar software de internet en los equipos de la institución ya que estos pueden contener virus dejando en riesgo los sistemas de la institución y datos.
5. Ningún funcionario deberá fumar, comer o beber en el puesto de trabajo ya que expone los equipos de cómputo a daños eléctricos o riesgo de contaminación sobre los dispositivos ya que pueden generar fallas tales como las siguientes.
   a. Migajas o sobras de comida en los teclados: genera una falla en que las teclas dejan de funcionar.
   b. Líquidos se pueden derramar en la superficie de los equipos: generando un corto en los mismos.

6. Ningún usuario puede trasladar, desconectar o conectar los equipos de cómputo sin la autorización del área de TIC's. Con esto se minimiza los posibles daños en los equipos por mala manipulación.
7. Ningún usuario debe modificar la configuración del Software Base (Sistemas Operativos, Programas antivirus, programas de mail) como tampoco modificar la configuración de los equipos de cómputo a través del Setup de la máquina; esto evita problemas de des configuración que pueden ocasionar conflictos tanto en el software como en el hardware
8. Los funcionarios deben pagar los equipos de cómputo al terminar la jornada laboral y al ausentarse del puesto de trabajo apagar o cerrar sesión en el sistema, esto evita el uso indebido de los equipos por parte de personas extrañas o ajenas al área, alarga la vida útil de las máquinas y contribuye al ahorro de energía eléctrica.

## 6. SANCIONES

El incumplimiento de estas políticas de seguridad, privacidad y reglamento de Seguridad Informática traerá consigo las consecuencias legales que apliquen a la normativa de la institución, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

1. Cualquier violación a la política o reglamento de Seguridad informática y Física de la institución deberá ser sancionada de acuerdo al Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la

normativa atinente y supletoria y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

2. Cuando se asume que la primera violación de las políticas de seguridad e informática es accidental o inadvertida, se debe hacer una amonestación. Una segunda violación sobre el mismo tema, hará que se envíe una carta al archivo del empleado. Una tercera violación, ocasionará la suspensión de trabajo por varios días sin pago. Una cuarta violación ocasionará el despido. Violaciones intencionales o a propósito sin importar el número de las mismas, puede resultar en acciones disciplinarias que deben llegar hasta el despido.
3. Hasta la culminación del contrato, los colaboradores no pueden retener o retirar desde las instalaciones de la institución cualquier información de la misma diferente a copias personales de correspondencia relacionada directamente con los términos y condiciones de su empleo. Cualquier otra información de la institución en custodia del trabajador que se retira, debe ser entregada al supervisor inmediato del trabajador en el momento de su salida.

4. En la terminación o expiración de su contrato, todos los contratistas, asesores y temporales deben entregar personalmente a su supervisor todas las copias de la información recibida de la institución o creada durante la ejecución del contrato. No deberán borrar información de los equipos, correo o drive.
5. En el evento en el que un empleado, asesor o contratista, se le termina su relación con la institución, el jefe inmediato o supervisor del trabajador es responsable por:
   a. Asegurarse de que toda la propiedad en custodia del trabajador sea regresada antes de que el trabajador deje la institución.

b. Notificar al área de las TIC's sobre el manejo de las cuentas del computador y correo utilizadas por el trabajador tan pronto como se conozca su retiro.
c. El área de TIC's revocará todos los privilegios relacionados con el trabajo de la persona que se retira.
d. El área de TIC's cambiará las claves de acceso a los correos de los funcionarios que terminan contrato, además de realizar una restauración del contenido de los correos (mensajes y drive).
e. Se eliminarán los accesos remotos y se crearán nuevas contraseñas para los equipos de cómputo.

## 7. BASE LEGAL

Lo expuesto en este documento está amparado en los acuerdos del Reglamento Interno de Trabajo, las normas, leyes y estatutos de la ley colombiana.

1. Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.
2. Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
3. Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se

encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.

4. Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
5. Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
6. ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.
7. ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.
8. Ley 962 DE 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
9. ISO/IEC TR 18044:2004: Ofrece asesoramiento y orientación sobre la seguridad de la información de gestión de incidencias para los administradores

de seguridad de la información y de los administradores de sistemas de información.

10. Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.