



# Función Pública



## Política de Operación

### Proceso de Tecnologías de la Información

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA

Versión 10  
Septiembre 2024



# Función Pública

Versión	Fecha de versión (aaaa-mm-dd)	Descripción del cambio
08	2021-04-23	Se ajustaron los capítulos: 5.5. Sobre los Derechos de Autor, Administración de Software y Licencias de Uso 5.9. Sobre los Bienes Informáticos
09	2024-09-26	Se ajustaron los capítulos: 5.2. Sobre la implementación y mantenimiento de Software 5.1 Sistemas de Información

## Contenido

1. Objetivo .....	3
2. Ámbitos de aplicación .....	3
3. Alcance.....	3
4. Responsabilidad de OTIC .....	3
5. Guías de acción del Proceso de Tecnologías de la Información .....	4
5.1. Sistemas de Información .....	4
5.2. Sobre la implementación y mantenimiento de Software.....	6
5.3. Sobre la implementación y mantenimiento de Infraestructura de TI .....	8
5.4. Sobre el uso de recursos de infraestructura de TI.....	8
5.5. Sobre los Derechos de Autor, Administración de Software y Licencias de Uso ...	9
5.6. Sobre Internet y Correo Electrónico Institucional Internet .....	11
5.7. De Aplicación por parte del usuario .....	12
5.8. Sobre las Medidas de Seguridad Física del Centro de Datos Interno .....	12
5.9. Sobre los Bienes Informáticos .....	13
5.10. Sobre el inventario de Bienes Intangibles.....	15
5.10.1. Sobre el ingreso de inventario de bienes intangibles .....	16
5.10.2. Sobre la dada de baja de bienes intangibles.....	17
5.10.3. Sobre el ajuste a información relacionada con los de Bienes Intangibles ...	18
5.10.4. Sobre conciliación del inventario de Bienes Intangibles.....	19
5.10.5. Sobre el Inventario de Activos de Información .....	19
5.11. De Aplicación por parte del usuario.....	20
5.12. Sobre la gestión de usuarios a nivel de base de datos.....	21
5.13. Lineamientos y acciones para construir contraseñas seguras.....	22
5.14. Sobre el acceso físico al centro de datos .....	23

## **1. Objetivo**

Brindar principios, lineamientos, parámetros y flujos de trabajo para la gestión de las tecnologías de la información y las comunicaciones en Función Pública y la implementación de proyectos estratégicos y de operación, que permitan obtener productos y servicios de TI acordes con las necesidades institucionales y sectoriales.

## **2. Ámbitos de aplicación**

La política de operación del Proceso de Tecnologías de la Información es aplicable a todos los procesos institucionales.

## **3. Alcance**

Estas políticas están dirigidas a las directivas, Servidores Públicos, contratistas, consultores, pasantes y personal vinculado a través de organizaciones que prestan servicios a la entidad, que laboran en las instalaciones de Función Pública y que utilizan las tecnologías de información y de comunicaciones propiedad del mismo.

## **4. Responsabilidad de OTIC**

La Oficina de Tecnologías de la Información y las Comunicaciones- OTIC es la responsable de establecer los lineamientos para la incorporación, uso y apropiación de las tecnologías de la información y las comunicaciones mediante el desarrollo de proyectos tecnológicos orientados al cumplimiento de los objetivos institucionales. Así mismo, es la responsable de gestionar de manera integral las tecnologías de la información en la entidad, prestando

servicios acordes a las necesidades de la misma, contribuyendo al desarrollo y al logro de las metas misionales, estratégicas y de apoyo.

El cumplimiento de la política de operación del proceso de tecnologías de la información y las comunicaciones es obligatorio y será compromiso de cada usuario acatar las directrices establecidas para el desarrollo de sus funciones.

Las excepciones a cualquier cumplimiento de la política de operación del proceso de tecnologías de la información y las comunicaciones deben ser aprobadas por el líder de Oficina de Tecnologías de la Información y las Comunicaciones y deben ser formalmente documentadas, registradas y revisadas.

## **5. Guías de acción del Proceso de Tecnologías de la Información**

### **5.1. Sistemas de Información**

- La Oficina de Tecnologías de la Información y las Comunicaciones debe asegurar que en el diseño e implementación de sus sistemas de información se incorporen funcionalidades que faciliten la generación de datos abiertos.
- La Oficina de Tecnologías de la Información y las Comunicaciones se encarga de impartir lineamientos en materia de tecnología para definir políticas, estrategias y prácticas que soportan la gestión de la entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones es el responsable de, elaborar el Plan Estratégico de Tecnologías de la Información y las Comunicaciones a nivel Institucional y Sectorial.
- La Oficina de Tecnologías de la Información y las Comunicaciones es el responsable de definir los estándares de datos, sistemas de información y seguridad informática de la entidad.



## Función Pública

- La Oficina de Tecnologías de la Información y las Comunicaciones el encargado de impartir lineamientos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información para la entidad,
- La Oficina de Tecnologías de la Información y las Comunicaciones debe propender por desarrollar los mecanismos necesarios para compartir su información haciendo uso del Modelo de Interoperabilidad definido por el Estado a partir de las necesidades de intercambio de información con otras entidades.
- Corresponde al proceso de Tecnologías de la Información disponer de la plataforma tecnológica, promover el uso adecuado de los recursos tecnológicos y brindar soporte especializado relacionado con tecnologías de la información.
- La Oficina de Tecnologías de la Información y las Comunicaciones debe definir, planificar, implementar y monitorear los recursos de software, hardware, redes y comunicaciones.
- Será el proceso de Tecnologías de la Información quien coordine la implementación de los Sistemas de Información, Aplicaciones, Portales y Micro sitios de la entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones es la encargada de investigar, evaluar, definir, aprobar y gestionar la adquisición y renovación de bienes y servicios tecnológicos de la Entidad, garantizando el cumplimiento de los lineamientos y políticas establecidas.
- La Oficina de Tecnologías de la Información y las Comunicaciones el encargado de dirigir y coordinar el análisis, diseño, construcción, documentación, implantación y mantenimiento de los sistemas, servicios y soluciones de TI.
- La Oficina de Tecnologías de la Información y las Comunicaciones identificar las necesidades de capacitación para fortalecer el uso y apropiación de TI en la entidad.
- Es compromiso de cada usuario de un computador, servicios y redes de la Entidad acatar las directrices establecidas para el desarrollo de sus funciones.



## Función Pública

- Los recursos informáticos y de comunicaciones solo podrán ser utilizados por los servidores, contratistas, pasantes y proveedores autorizados por Función Pública y en desarrollo de las labores que se determinen para tal fin.
- Los servicios informáticos se brindarán en función de los recursos disponibles en Función Pública.
- Todo proyecto, solicitud de compra, adquisición actualización o baja de recursos de informática y comunicaciones debe contar con la respectiva autorización y concepto técnico del Proceso de Tecnologías de la Información.
- La Oficina de Tecnologías de la Información y las Comunicaciones mantendrá la confidencialidad de los datos almacenados en los sistemas de información. Sólo se permitirá el acceso a información propia de los usuarios cuando sea solicitado de manera formal por una autoridad competente, con la respectiva justificación.
- Toda persona que para el desempeño de sus funciones utilice o tenga acceso a los bienes o servicios informáticos que ofrece la Institución deberá observar y tener en cuenta lo prescrito en la presente política.

### **5.2. Sobre la implementación y mantenimiento de Software**

- La Oficina de Tecnologías de la Información y las Comunicaciones es responsable de liderar la implementación, mantenimiento (correctivo, preventivo) y configuración de todos los sistemas de información, aplicaciones y servicios de tecnología de la entidad.
- La Oficina de tecnología de la Información y las Comunicaciones es el área responsable de realizar el análisis de la necesidad, viabilidad técnica y presupuestal, definición técnica de la solución y gestionar su implementación. Lo anterior, con el apoyo del líder del área solicitante y el grupo responsable de la adquisición de bienes y servicios de la entidad.



## Función Pública

- Cuando un área requiera implementar una aplicación y/o sistemas de información, debe realizar la solicitud al jefe o coordinadores de la Oficina de Tecnologías de la Información y las Comunicaciones para que sea analizado.
- Solo la Oficina de Tecnologías de la Información y las Comunicaciones podrá adquirir, desarrollar e implementar sistemas de información.
- Todo desarrollo, invención o aplicación realizada para la Función Pública, será propiedad de la Entidad.
- Todo software y/o aplicación adquirida por la entidad, debe estar debidamente registrada ante la Oficina de Registro de la Dirección Nacional de Derecho de Autor y se debe contar con la autorización de comercialización del dueño del software.
- Para el caso de desarrollos a la medida, el contratista debe entregar la cesión de los derechos patrimoniales a la entidad.
- Cuando se requiera realizar mantenimiento a una aplicación y/o sistemas de información, se debe realizar la solicitud por medio de la herramienta de mesa de servicio – Proactiva Net.
- La adquisición, implementación, desarrollo y mantenimiento software debe ser estructurado teniendo en cuenta cada una de las etapas del ciclo de vida del software (análisis, diseño, desarrollo, pruebas, puesta en producción y mantenimiento).
- Todos los servicios de TI deben estar parametrizados en la herramienta de mesa de servicio, especificando los Acuerdos de Nivel de Servicio (ANS) y responsables de la atención del servicio. Para los casos que aplique se deben definir los Acuerdos de Niveles de Operación (OLAS).
- Los usuarios de los sistemas de información de Función Pública serán los responsables del contenido y actualización permanente de los datos relacionados con su gestión.
- El control de acceso a los sistemas de información será determinado por cada uno de los administradores funcionales del sistema.

- La Oficina de Tecnologías de la Información y las Comunicaciones es el encargado de la implementación de la gestión de parches para actualizar el software y tener un control y visibilidad total sobre el software instalado en la red, esta actividad se puede realizar manualmente o mediante una solución automatizada.

### **5.3. Sobre la implementación y mantenimiento de Infraestructura de TI**

- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de administrar la infraestructura de TI de propiedad de la entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones es la responsable de hacer seguimiento a los servicios adquiridos a través de terceros y de gestionar los incidentes y peticiones que se presenten ante los proveedores de los servicios, alineado con las obligaciones del contrato.
- El Proceso de Tecnologías de la Información establecerá los mecanismos para la gestión de copias de seguridad, que permitan recuperar los datos y configuración de los sistemas.
- Establecerá y validará las condiciones de la protección física y ambiental de las copias de respaldo.

### **5.4. Sobre el uso de recursos de infraestructura de TI**

- Se establece que los computadores de escritorio, computadores portátiles y dispositivos móviles pertenecientes a la entidad, pueden hacer uso de los recursos de red a través de los siguientes medios:
  - Cable de red
  - Red inalámbrica
- Lo anterior solo aplica para usuarios previamente autorizados en el directorio activo.



## Función Pública

- Se establece que los computadores de escritorio, computadores portátiles y dispositivos móviles propiedad de terceros, solo pueden hacer uso de los recursos de la red (internet) utilizando la red cableada e inalámbrica de invitados.
- Cuando la infraestructura tecnológica de la entidad requiera ser utilizada por terceros, se deberá realizar la solicitud utilizando la herramienta de mesa de servicio, previa autorización del jefe del área a la que pertenezca.
- El uso de recursos de red mediante acceso remoto –Red privada virtual VPN-, solo se habilita previa solicitud a través de la herramienta de mesa de servicio, previa autorización del jefe del área a la que pertenezca.
- El usuario deberá utilizar la cuenta asignada, para el acceso a los servicios y recursos tecnológicos a los que tenga permiso.
- El usuario hará uso exclusivo de los recursos disponibles a través de la red de la entidad para el cumplimiento de las funciones asignadas. La entidad se reserva el derecho de monitorear las actividades realizadas a través de la red de la entidad.
- El Proceso de Tecnologías de la Información administra los servicios de la red de datos institucional de manera exclusiva, con el personal del área responsable de esta función y en los casos necesarios, con la participación de proveedores autorizados.

### **5.5. Sobre los Derechos de Autor, Administración de Software y Licencias de Uso**

- El Proceso de Tecnologías de la Información definirá los estándares y versiones de software necesarios para el desarrollo y operación de los sistemas de información de Función Pública.
- Se establece que el software instalado en la infraestructura tecnológica de la entidad debe estar debidamente licenciado. Se prohíbe la instalación de software no licenciado (juegos y software libre).



## Función Pública

- Para el caso de requerir instalar software libre se deberá realizar la solicitud utilizando la herramienta de mesa de servicio, previa autorización del jefe del área, indicando la finalidad de uso, periodo de utilización y autorizaciones del fabricante.
- Para el caso de requerir instalar software licenciado por Función Pública, se deberá realizar la solicitud por la herramienta mesa de servicio, para lo cual el grupo de mesa de servicio deberá revisar que existen licencias disponibles antes de su instalación.
- En caso de requerir que un servidor público tenga administración total del computador de escritorio y/o computador portátil de propiedad de la entidad para el cumplimiento de sus funciones, deberá realizar la solicitud utilizando la herramienta de mesa de servicio, previa autorización del jefe del área. En dicha solicitud se deberá indicar el tiempo requerido con permisos de administrador. Una vez se cumpla el tiempo solicitado, el rol de administrador será revocado previa revisión del software instalado. En caso de encontrar software no autorizado, se procederá a su desinstalación y notificación del hallazgo al jefe del área y control interno por incumplimiento de esta política.
- El licenciamiento de los computadores de escritorio, computadores portátiles y dispositivos móviles propiedad de terceros o del personal de la entidad para uso personal, no es responsabilidad de la entidad. Por tanto, la persona dueña o responsable del elemento ingresado a la entidad deberá garantizar la legalidad del licenciamiento para cada producto instalado. En caso de incumplimiento de las normas que protegen el software, dicha persona será el único responsable.
- Se establece como software básico obligatorio para computadores de escritorio, computadores portátiles y dispositivos móviles de propiedad de la función pública los siguientes: (Windows Profesional, Office Standard, Power BI Desktop, Skype Empresarial, OneDrive Corporativo, Antivirus).
- Se establece como Software básico Free que pueda ser instalado en los computadores de escritorio, computadores portátiles y dispositivos móviles de



## Función Pública

propiedad de Función Pública los siguientes: (Acrobat Reader DC, Bizagi Process Modeler, FastStone Image Viewer, Skype, AdobeFlash, CCleaner, GoogleChrome, Mozilla Firefox, Java, FreeMind, PDFCreator, Winrar, VLC media player, Movie Maker).

- Se establece como software básico mínimo para computadores de escritorio, computadores portátiles y dispositivos móviles de propiedad de terceros los siguientes: Office y Antivirus.
- Cualquier instalación de software o hardware deberá ser avalado y autorizado por el Proceso de Tecnologías de la Información.
- Se prohíbe el almacenamiento de cualquier material protegido por Derechos de Autor (material de audio, video, gráfico, etc.) sin su respectiva licencia.

### 5.6. Sobre Internet y Correo Electrónico Institucional Internet

- La entidad proveerá el canal de comunicación con Internet.
- Los accesos a las páginas Web a través de los navegadores estarán sujetas a las políticas de acceso y control al proxy con fines restrictivos para la consulta de páginas indebidas (pornografía infantil, trata de personas o contrabando) con la correspondiente implementación de filtros de contenido y de navegación instalados en la red de la entidad.
- El uso del internet está sujeto a las necesidades propias de sus funciones u obligaciones, por lo tanto, deberá hacer uso racional y apropiado del mismo.
- Se debe hacer buen uso de las agrupaciones que contiene la libreta de direcciones.
- El usuario hará buen uso del espacio de almacenamiento asignado para su cuenta de correo y aplicará los lineamientos establecidos por el Proceso de Tecnología de la Información para su administración.
- La creación y eliminación de las cuentas de correo están a cargo del Grupo de Gestión Humana para servidores públicos y pasantes que laboren en la entidad

y el Grupo de Gestión Contractual para el caso de contratistas. Lo anterior se debe realizar a través de la herramienta de mesa de servicio.

### **5.7. De Aplicación por parte del usuario**

- Las tarjetas inteligentes, tokens y llaves asignados a los usuarios, los cuales permiten acceder a los servicios, sistemas, redes y ubicaciones físicas de recursos informáticos son personales e intransferibles. Su uso, administración y reserva será responsabilidad de cada usuario.
- Los usuarios deben reportar cualquier anomalía en los equipos o impresoras, a través de la herramienta de mesa de servicio. Bajo ninguna circunstancia el usuario debe manipular los equipos de cómputo ni sus archivos y software asociado. Esta actividad sólo la debe hacer el personal autorizado.
- Los usuarios deberán vacunar la información proveniente de medios de almacenamientos externos antes de su utilización en los equipos de cómputo de la Entidad.
- Todos los equipos que no estén siendo utilizados, deben permanecer bloqueados mientras los usuarios se encuentren ausentes de su área de trabajo. Cuando el usuario abandone el área de trabajo, previamente deberá finalizar todos los procesos que esté desarrollando y apagar el equipo. Solo en casos excepcionales el equipo de cómputo podrá permanecer encendido, para estos casos se debe notificar al Grupo de Gestión Administrativa indicando el motivo y el tiempo que deberá permanecer encendido.

### **5.8. Sobre las Medidas de Seguridad Física del Centro de Datos Interno**

- Se verificará que las instalaciones físicas donde se ubiquen los bienes informáticos cumplan con las condiciones mínimas requeridas para su adecuada



## Función Pública

conservación y funcionamiento (temperatura, electricidad, mobiliario, identificación de rutas de evacuación etc.)

- El centro de Cómputo dispondrá de piso de placas extraíbles a fin de permitir el manejo de cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos.
- El Centro de Cómputo contará con: Extintor, Sistema de Aire acondicionado, cableado bajo tierra o en conductos protegidos y no almacenará elementos combustibles.
- Se generarán y actualizarán los planos que contengan los recursos de tecnología que proveen los servicios de conectividad y otros. Estos deben incluir los inventarios y esquemas de las redes y equipos de conectividad asociados, así como los planos de cableado estructurado de la Entidad.
- Se mantendrán los servidores de red y los equipos de comunicaciones en cuartos cerrados o en gabinetes con llaves y con restricciones de acceso a personal no autorizado.
- Se procurará que los accesos de entrada física (puertas, ventanas, paredes de vidrio, ventilación, etc.) existentes en áreas informáticas no estén expuestos a violación accidental o intencional, igualmente los controles físicos limitarán el acceso solo al personal autorizado.

### 5.9. Sobre los Bienes Informáticos

- La infraestructura tecnológica de la entidad deberá estar conectada a los puntos de corriente regulada y a estas tomas no se deberán conectar otro tipo de aparatos eléctricos tales como aspiradoras, brilladoras, radios, cocinetas, entre otros.



## Función Pública

- Todo el equipo de cómputo que esté o sea conectado a la red de la Entidad, o aquel que en forma autónoma se tenga y que sea propiedad de la institución, debe sujetarse a las normas y procedimientos establecidos.
- El proceso de tecnologías de la información es el encargado de planificar la renovación y/o actualización de la infraestructura tecnológica de la entidad considerando tanto los requerimientos actuales, requerimientos futuros y tecnología disponible en el mercado.
- El proceso de tecnologías de la información es el responsable de establecer los lineamientos para el soporte y mantenimiento de los recursos informáticos de la Entidad.
- El Grupo de Gestión Administrativa es la responsable de atender la mesa de servicio de primer nivel, acorde a los lineamientos que la Oficina de Tecnologías de la Información y las Comunicaciones establezca.
- Mantendrá en coordinación con el Grupo de Gestión Administrativa registro de todos los equipos propiedad de Función Pública y de los responsables de su uso.
- El acceso a los servidores de la entidad será restringido; excepto para el personal del proceso de tecnologías de la información encargado de las labores de administración de la infraestructura tecnológica.
- Mantendrá en coordinación con el Grupo de Gestión Administrativa el inventario y control de las licencias de software adquiridas por la Entidad.
- La Oficina de Tecnologías de la Información y las Comunicaciones es el responsable de la custodia y control de las licencias de software, así como de la solicitud de dada de baja de las mismas.
- Para los procesos de adquisición de computadores de escritorio y portátiles que adelante Función Pública: cuando las máquinas se adquieran con licenciamiento de sistema Operativo, éste viene preinstalado de fábrica y a nombre de un tercero (distribuidor); dichas licencias no serán tenidas en cuenta en el inventario de activos intangibles y se tomaran como mayor valor de la máquina adquirida.

El grupo de gestión administrativa será el encargado de reinstalar el sistema operativo de acuerdo a la disponibilidad de licencias con las que cuente la entidad, previa autorización de la Oficina de Tecnologías de la Información y las Comunicaciones.

- Cuando las máquinas se compren sin sistema operativo, el grupo de gestión administrativa será el encargado de proceder a instalar el sistema operativo previamente adquirido y debidamente licenciado por la Oficina de Tecnologías de la Información y las Comunicaciones. Para el proceso de adquisición de licenciamiento de software Microsoft, las licencias deben quedar registradas en la plataforma de Microsoft a nombre de Función Pública.

#### **5.10. Sobre el inventario de Bienes Intangibles**

- Los bienes intangibles corresponden a software adquirido o desarrollad o y deben ser tratados como elementos contables, aunque no tengan apariencia física. Es decir, que los bienes intangibles son tratados de la misma manera que un bien tangible.
- Teniendo en cuenta que el registro del licenciamiento de Microsoft se realiza utilizando los datos del supervisor del contrato, se establece que la cuenta de correo a registrar como parte de la información del supervisor debe ser [adminlicencias@funcionpublica.gov.co](mailto:adminlicencias@funcionpublica.gov.co). Lo anterior, con el fin de tener consolidado el inventario de licencias en la Plataforma de Microsoft.
- Se dispone una la herramienta de Gestión de Servicios de TI – Proactiva NET®, donde se tiene configurada la categoría licenciamiento para realizar el ingreso, dada de baja y ajustes de bienes intangibles adquiridos o desarrollados por Función Pública.

### 5.10.1. Sobre el ingreso de inventario de bienes intangibles

- Se debe tener en cuenta que la asignación de placa de inventario se asigna por producto.
- El tipo de licenciamiento de software que ingresa al almacén es el siguiente: por procesador, usuario, módulo, suscripción, cliente, servidor y core. Si se presenta un tipo de licenciamiento no contemplado en la anterior lista, se debe realizar una reunión con el jefe de la oficina de TIC y coordinador del grupo de servicios de TI para revisar el caso.
- Se deberá anexar la factura y recibo a satisfacción de la licencia adquirida.
- Una vez diligenciada la información, Proactivanet asigna el caso al profesional de la oficina de TIC encargado de revisar la información registrada.
- El responsable de almacén:
  - Revisa la información registrada por el supervisor del contrato, en caso de presentar inconsistencias se devuelve al supervisor del contrato.
  - Se procede al registro en el Sistema de Inventarios.
  - Se genera el registro de ingreso.
  - Se registra el número de placa de inventario en Proactiva Net y se anexa el registro de ingreso a almacén.
  - Se reasigna a la Oficina de TIC.
- El supervisor revisa que el registro de ingreso a almacén corresponda a la información del bien intangible, si es correcta se resuelve el caso, si existe alguna inconsistencia se devuelve al almacén para su respectivo ajuste.
- El supervisor del contrato, debe descargar el registro de ingreso al almacén y anexarlo a la cuenta de cobro para su respectivo pago.

### 5.10.2. Sobre la dada de baja de bienes intangibles

- Para dar de baja un bien intangible, el supervisor o el responsable de la licencia debe utilizar la plantilla de “dar de baja bienes intangibles (software)”, a través de la herramienta mesa de servicio Proactiva Net.
- El concepto técnico debe ser claro y completo, para ello se debe indicar si la baja se da por obsolescencia, por fin del tiempo de licenciamiento, o cualquier motivo. Por ejemplo: Por finalización de la vida útil, se solicita dar de baja la licencia de software denominado [nombre de la licencia], identificado con placa de inventario [número placa de inventario] y la cual fue adquirida mediante contrato [numero/año del contrato] suscrito con la firma [nombre del contratista], por un tiempo de [años - meses].
- Una vez diligenciada la información, Proactiva Net asigna automáticamente el caso al profesional de la oficina de TIC encargado de revisar la información registrada. Si existe alguna inconsistencia se devuelve al supervisor por encargado de la licencia.
- La solicitud se debe remitir al coordinador del grupo de servicios de TI para su aprobación, la cual debe quedar registrada en la opción investigación de la plantilla de “dar de baja bienes intangibles (software)”, a través de la herramienta mesa de servicio Proactiva Net, para el caso asignado.
- Asignar la solicitud al encargado del Grupo de Gestión Administrativa – almacén para formalizar la dada de baja del bien intangible.
- La solicitud de dada de baja permanece abierta hasta que se realice la baja del bien intangible (egreso de los bienes del inventario), teniendo en cuenta que se debe:
  - En comité de sostenibilidad contable se verifica y se aprueba dar de baja el bien o bienes intangibles solicitados por la Oficina de TIC.

- Se elabora el acta de inspección ocular, donde se verifica las solicitudes de dada baja con las respectivas justificaciones, la cual es firmada por los integrantes del comité.
  - Se elabora la resolución de baja y posterior a la firma de la resolución
  - El área de almacén procede a sacar por medio de una baja los intangibles solicitados.
- 
- Una vez se cuenta con la resolución de egreso de bienes, se anexa este documento a la solicitud de Proactiva Net y se cierra dicha solicitud.

### **5.10.3. Sobre el ajuste a información relacionada con los de Bienes Intangibles**

- EL supervisor del contrato o encargado del bien intangible, puede solicitar ajustes a la información asociada, para ello debe diligenciar la información, a través de la plantilla “solicitud ajustes bienes intangibles (software)”, a través de la herramienta mesa de servicio Proactiva Net.
- El concepto técnico debe ser claro y completo, de tal forma que se entienda la necesidad de la solicitud. Por ejemplo: se solicita la unificación de licencias, teniendo en cuenta la solicitud de registro a almacén número [caso Proactiva Net] donde se indica que es una licencia para 50 usuarios.
- Si se requiere el cambio de vida útil, se debe tener en cuenta que la solicitud se debe realizar cuando quede al menos 6 meses de vida útil. Este ajuste tiene implicaciones contables, motivo por el cual solo en casos estrictamente necesarias se debe solicitar.
- Una vez diligenciada la información en la herramienta Proactiva Net, la solicitud es asignada automáticamente al profesional de la oficina de TIC encargado de revisar la información registrada. Si existe alguna inconsistencia se devuelve al supervisor por encargado de la licencia.



## Función Pública

- Asignar la solicitud al encargado del Grupo de Gestión Administrativa – almacén para formalizar el ajuste del bien intangible.
- Almacén resuelve el caso, solo hasta que se realice efectivamente el ajuste en el sistema de inventarios y se anexe el reporte del bien intangible actualizado.

### 5.10.4. Sobre conciliación del inventario de Bienes Intangibles

- La conciliación de inventario de software o bienes intangibles se debe realizar cada cuatro (4) meses entre la oficina de TIC y el Grupo de Gestión Administrativa – Almacén.
- El Grupo de Gestión Administrativa – Almacén, envía al coordinador del grupo de servicios de TI – OTIC, el inventario generado desde el sistema de inventarios, el listado de bienes intangibles (controlables y no controlables) tres semanas antes de la reunión cuatrimestral de conciliación.
- La oficina de TIC debe revisar el inventario de los bienes intangibles como máximo dos semanas después de recibido el inventario.
- Si la oficina de TIC requiere realizar una solicitud de ajuste o encuentra una inconsistencia se realiza la solicitud a través de la herramienta mesa de servicio Proactiva Net, con la plantilla “solicitud ajustes bienes intangibles (software)”.
- Como resultado de la reunión de conciliación de intangibles, se debe dejar como constancia el acta.
- El Grupo de Gestión Administrativa debe informar al Grupo de Gestión Financiera las novedades presentadas durante la conciliación.

### 5.10.5. Sobre el Inventario de Activos de Información

- Una vez realizada la conciliación de bienes intangibles y con la información de bienes tangibles entregada por el Grupo de Gestión Administrativa se debe revisar el inventario de activos de información.

- De presentarse alguna novedad sobre los activos de información se procede a actualizar la matriz y remitir al Grupo de Gestión Documental y a la Oficina Asesora de Planeación

#### **5.11. De Aplicación por parte del usuario**

- Para acceder a los recursos de infraestructura de TI, los usuarios deben contar con una cuenta de correo y una clave de acceso, la cual es confidencial e intransferible. El dueño de la cuenta es responsable de mantener la confidencialidad de la contraseña, de hacer uso adecuado de la misma y de responder sobre todas las actividades que ocurran bajo su cuenta.
- Queda prohibido al usuario prestar su cuenta institucional a otra persona o utilizarla para fines distintos al cumplimiento de sus funciones.
- Los usuarios deben velar por la salvaguarda de las contraseñas asignadas para el ingreso a las distintas aplicaciones y/o servicios de TI y se hace responsable por todas y cada una de las acciones que se hagan con su usuario.
- Los usuarios tendrán derecho a la confidencialidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad institucional, así como para responder ante quejas sobre contenidos que violen los derechos de terceras personas.
- Todos los documentos creados e información generada en los sistemas de información y bienes informáticos de la entidad son propiedad de Función Pública, y por lo tanto se prohíbe borrarlos en el momento de retiro de la Entidad.
- No está permitido obtener copias de archivos, códigos, contraseñas o información ajena, así mismo suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento del titular de la cuenta.

## 5.12. Sobre la gestión de usuarios a nivel de base de datos

- La solicitud de creación, modificación, inactivación o retiro de cuentas de usuario debe realizarse por el jefe de la Oficina de Tecnología, el coordinador del grupo de Servicios de Información, el coordinador del grupo de Proyectos Estratégicos y el coordinador del grupo de Servicios de TI, mediante la herramienta de mesa de servicio
- /Servicios Especializados TI / Base de Datos / Creación de usuarios. Solicitud que debe realizarse cuando se presente cualquier novedad administrativa (ingreso, traslado, retiro, licencia y cambio de funciones de un servidor público y/o contratista).
- Antes de proceder a la creación de usuarios, se debe tener el acuerdo de confidencialidad debidamente firmado y anexarlo escaneado a la solicitud.
- La solicitud debe contener la siguiente información: nombre de la base de datos, tablespace, schema, ambiente (desarrollo, pruebas, pre - producción, producción), privilegios que se le deben asignar al usuario (sobre objetos, del sistema, sobre roles) y tipo de autenticación.
- Las cuentas de usuario de Base de Datos son de carácter confidencial y no pueden ser compartidas, cualquier mal uso de la cuenta será responsabilidad de la persona
- a la que se le asignó, no debe utilizar cuentas genéricas. Es responsabilidad de cada servidor público y/o contratistas hacer buen uso del usuario de base de datos.
- La configuración y administración las cuentas de usuario de base de datos es responsabilidad del Administrador de Base de Datos de la entidad, el cual debe llevar el registro de las cuentas de usuario por base de datos: datos del usuario, fecha de creación, fecha de actualización, fecha de eliminación, servidor público que realizó la solicitud.

- El uso de los privilegios dados a cada usuario puede ser auditado cuando se considere necesario o por solicitud explícita del responsable técnico y/o funcional del sistema de información y/o la aplicación correspondiente.

### **5.13. Lineamientos y acciones para construir contraseñas seguras**

- Se deben utilizar al menos 8 caracteres para crear la clave, que sea de fácil recordación y se pueda escribir rápidamente.
- Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales (¡! " # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~). Al crear una contraseña se recomienda seleccionar palabras sin sentido pero que sean pronunciables, puede combinar números o letras e introducir alguna letra mayúscula. Así mismo, puede crear contraseñas eligiendo la primera letra cada una de las palabras que componen una frase, una canción o una película (ejemplo: para la película "Piratas del caribe: En el fin del mundo (2007)" la clave quedaría Pdc: Eefdm2007).
- Evitar utilizar secuencias de teclado o repetición de caracteres (ejemplo: qwerty, asdf, 1234, 98765, 111222).
- No escribir la contraseña en un papel o documento, ni guardarla en documentos de texto en un dispositivo electrónico.
- No se deben utilizar palabras que no estén registradas en diccionarios o en ningún idioma.
- Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.
- Por seguridad, las contraseñas deben ser cambiadas con cierta regularidad.



## Función Pública

- No utilizar información personal en la contraseña: nombre del usuario, nombre de familiares, apellidos, fecha de nacimiento, apodos, mascotas, número de identificación personal y teléfono entre otros.
- No enviar nunca la contraseña por correo electrónico o en mensajes de texto.
- No mencionar las contraseñas en conversación o comunicación de cualquier tipo.
- Cambiar las contraseñas por defecto proporcionadas por desarrolladores y/o fabricantes.

### 5.14. Sobre el acceso físico al centro de datos

- El acceso al centro de datos será controlado a través de tarjeta de proximidad o control biométrico (huella).
- No deben almacenarse en el centro de datos materiales inflamables o peligrosos.
- El centro de datos debe mantenerse cerrado, limpio y ordenado.
- Solo personal autorizado puede ingresar al centro de datos. La autorización de entrada al centro de datos está a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.
- Para los servidores públicos, contratistas u otras personas que no estén autorizados para ingresar al centro de datos y requieran un permiso temporal, se deberá realizar la solicitud por el jefe del área a través de la herramienta de mesa de servicio indicando: empresa, área, nombres completos, número de identificación, motivo de la solicitud de acceso, rango de fechas y horario.
- Toda persona con acceso temporal al centro de datos debe estar acompañada por personal con autorización permanente. En ningún caso puede permanecer solo en las instalaciones del centro de datos.
- Al finalizar cualquier actividad en el centro de datos, se debe asegurar el orden, la limpieza y garantizar que las puertas queden cerradas y la luz apagada.



## Función Pública

- Está prohibido el ingreso de personal que esté bajo los efectos del alcohol, drogas o cualquier sustancia alucinógena.
- Está prohibido ingresar al centro de datos alimentos, bebidas, tabaco, armas corto punzantes o de fuego, materiales inflamables, materiales corrosivos, materiales radioactivos y materiales electromagnéticos.
- Está prohibido intervenir sensores, redes, cableados, accesos, equipos, cámaras u otros dispositivos que no sean de directa relación con los trabajos que están programados y autorizados.
- Está prohibido dañar, modificar, adulterar, conectar y desconectar la infraestructura dispuesta en el centro de datos, que pueda afectar el funcionamiento o servicios de la entidad.

# Política de Operación

Versión 09  
Proceso de Tecnologías de la Información  
Septiembre de 2024