**ESE SANTIAGO DE TUNJA**

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

## 1. OBJETIVOS

### 1.1. Objetivo general

Concientizar sobre el uso adecuado de los sistemas de información y los recursos tecnológicos de la ESE Santiago de Tunja, por parte de todos los funcionarios; preservando, protegiendo y administrando de forma correcta la información y los medios electrónicos utilizados para su manipulación y procesamiento.

### 1.2. Objetivos específicos

- Socializar a los funcionarios de la ESE Santiago de Tunja acerca de las políticas de seguridad y privacidad de la información, con el fin de minimizar las amenazas que puedan afectan el buen desarrollo del proceso de la entidad frente a seguridad de la información.
- Aplicar las políticas de seguridad a el equipamiento tecnología de la entidad.

## 2. ALCANCE

El presente documento tendrá como alcance, el brindar las políticas y conceptos técnicos aplicables a la seguridad y privacidad e la información con el objetivo de estar alineados frente a los lineamientos estratégicos del sector TI, que busca el uso responsable de las telecomunicaciones.

## 3. MARCO NORMATIVO

- LEY 527 DE 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."
- LEY ESTATUTARIA 1266 DE 2008: "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la

financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.".

- LEY ESTATUTARIA 1581 DE 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales.".
- LEY 1712 DE 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- DECRETO 1499 DE 2017: "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
- DECRETO 612 DE 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.".
- Decreto 1008 del 14 de junio de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

## 4. TERMINOS Y DEFINICIONES

- **COPIA DE SEGURIDAD**: Es el almacenamiento de las bases de datos y/o archivos residentes en los servidores y equipos propiedad de la Empresa, en un dispositivo de almacenamiento que además de garantizar su integridad y oportunidad, para realizar procesos de recuperación de información en los casos de siniestralidad, son un mecanismo de análisis histórico de operaciones.
- **RESTAURACION**: Acción de tomar una copia de seguridad y emprender las actividades encaminadas a restablecer un archivo o documento con corte a una fecha determinada.

- **SERVIDOR**: Es un computador cuyo propósito es proveer datos o servicios de modo que otros computadores los puedan utilizar y administrar las bases de datos en las que se almacena la información de los procesos que cuentan con aplicativos residentes en el.
- **CAMPO:** Unidad básica de una base de datos.
- **ARCHIVO:** Es un elemento de información conformado por un conjunto de registros. Es decir que estos registros a su vez están compuestos por una serie de caracteres o bytes
- **REGISTRO:** Es el conjunto de información referida a una misma persona u objeto. Un registro vendría a ser algo así como una ficha.
- **BASE DE DATOS:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
- **SISTEMAS GESTORES DE BASES DE DATOS**: SGBD, Permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada.
- **DISCO DURO:** Es un dispositivo de almacenamiento de datos que emplea un sistema de grabación magnética externa para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada.
- **DVD:** Es un dispositivo de almacenamiento óptico cuyo estándar surgió en 1995. Sus siglas corresponden con *Digital Versatile Disc*[1] en inglés (*disco versátil digital*). Un dispositivo de almacenamiento masivo de datos cuyo aspecto es idéntico al de un disco compacto, aunque contiene hasta 15 veces más información y puede transmitirla a la computadora unas 20 veces más rápido que un CD-ROM.
- **CONFIDENCIALIDAD:** es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin.

- **INTEGRIDAD:** es la preservación de la información completa y exacta.
- **DISPONIBILIDAD:** es la garantía de que el usuario accede a la información que necesita en ese preciso momento.

## 5. ROLES Y RESPONSABILIDADES

**Líder sistemas:** identificar las falencias y fallas que se presenten en los sistemas de información e infraestructura tecnológica de la entidad , realizar los ajustes que sean necesarios para corregir o evitar que estos puedan afectar negativamente el buen funcionamiento de los recursos informáticos , además de hacer cumplir las políticas de seguridad y privacidad de la información mediante auditorias que permitan el levantamiento de planes de mejora ,promover y divulgar las políticas para minimizar los riegos y proveer los recurso que en materia de seguridad de la información para el cumplimiento de las mismas.

**Técnico mantenimiento:** apoyar, conocer y aplicar las políticas de seguridad de la información, así como apoyar los procesos, toma de decisiones y dar solución frente a cualquier eventualidad que pueda ser una amenaza para la entidad en materia de seguridad e integridad de la información.

**Usuarios:** conocer y poner en práctica las políticas de seguridad y privacidad de la información, además de realizar buenas prácticas para el buen uso de los recursos tecnológicos de la entidad e informar sobre cualquier anomalía que pueda afectar el correcto funcionamiento de los recursos informáticos de la entidad o cualquier incidente que sea detectado en el desarrollo de las actividades laborales diarias.

## 6. DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD

### 6.1. Acceso a la información

Los funcionarios de la ESE Santiago de Tunja que se encuentra vinculados laboralmente a la entidad solo podrán tener acceso a la información que sea estrictamente de sus áreas funcionales o que sea correlacionada para complementar las actividades afines del área, es responsabilidad del comité de seguridad de la información conceder el acceso a la información de acuerdo al cargo o trabajo que se encuentre realizando. Una vez el funcionario se encuentre desvinculado de su cargo este deberá inmediatamente dejar de acceder a la información que en primera medida se le fue concedida para la realización de actividades, así como servicios en red y correos corporativos por otro lado cualquier información generada procesada y contenida en los equipos es de estricta propiedad de la entidad.

### 6.2. Seguridad de la información

Cada funcionario debe velar por la integridad de la información, confidencialidad, disponibilidad y fiabilidad que tenga a su cargo, además de garantizar la custodia de la información especialmente si dicha información ha sido categorizada como confidencial o critica, evitando que personal no autorizado pueda acceder, borrar, modificar o copiar cualquier tipo de archivo en mención. para ello es indispensable que los equipos tengan asignado un usuario y contraseña del equipo de trabajo para reducir el riego de acceso por terceros además de realizar el bloqueo del equipo cada que exista algún tipo de desplazamiento del área de trabajo para evitar y prevenir un acceso no autorizado.

### 6.3. Seguridad sistemas de información

la red de internet solo deberá ser utilizada para fines laborales, no se encuentra permitido el uso de los recursos para el ingreso de páginas: pornográficas, radios online, programas de televisión, plataformas de videojuegos,

apuestas, compras en línea, redes sociales, sitios de material bélico, drogas, sitios maliciosos, descarga de software gratuito, entre otros.

Cualquier acceso no autorizado a los sitios mencionados por medio de navegadores no permitidos o en modo incognito en la entidad, será reportado por el comité de seguridad de la información a los entes de control de la ESE Santiago de Tunja quienes a su vez realizaran el seguimiento de caso y desarrollaran medidas necesarias para el cumplimiento de las políticas de seguridad e integridad de la información.

Contraseñas

- Hacer claves de una longitud mínima de 8 caracteres. Los caracteres vuelven a la contraseña más robusta.
- Realizar combinaciones alfanuméricas. Estas son más difíciles de descubrir, teniendo en cuenta las diversas posibilidades de combinación de los caracteres.
- Utilizar distintas claves para cada servicio. De esta manera, si la contraseña es revelada, será más difícil para el atacante acceder al resto de las plataformas del usuario.
- Evitar palabras comunes. Quienes conocen de informática pueden revelar una clave en cuestión de segundos.
- Cambiar periódicamente las claves. Esto aumenta el nivel de seguridad de las credenciales.
- **Finalmente, tres estrategias para recordar las diferentes claves a lo largo del tiempo:**
- Cambiar las vocales por números. Por ejemplo, “Mi Clave es segura”: M3 Cl1v2 2s s2g5r1.
- Utilizar reglas mnemotécnicas, como elegir la primera letra de cada una de las palabras de una frase fácil de recordar. Por ejemplo, “Mi Clave es segura”: MCe10vs.

- Claves basadas en un mismo patrón. Por ejemplo, añadir al final las iniciales cada red social: MCe10vFB (Facebook); MCe10vTR (Twitter); MCe10vsGM (Gmail)[1]

### 6.4. Seguridad en recursos informáticos

Los usuarios que utilicen los servicios informáticos deben establecer claves seguras de ingreso a los distintos recursos informáticos y cambiar periódicamente las credenciales de acceso para evitar que terceros puedan acceder a información de la entidad.

Los sistemas de información como aplicaciones de bases de datos, servidores y aplicativos de la entidad, deberán contar con roles establecidos para minimizar el riesgo de acceso por terceros, además de restringir el acceso a perfiles de administrador a quienes no cumplan dicha función.

La entidad debe tener definido los perfiles de usuarios de acuerdo a la función asignada dentro del cargo al cual es asignado.

Toda la información que sea sensible, critica o valiosa para la entidad deberás ser protegida mediante controles de acceso para garantizar que pueda ser modificada, publicada o borrada.

### 6.5. Seguridad en comunicaciones

La segmentación IP, topologías de redes, configuraciones e información relacionada con la estructura interna de redes de comunicaciones de la entidad deberá ser tratada de manera confidencial.

[1] 1Fuente: https://www.lavoz.com.ar/tecno/diez-recomendaciones-para-crear-una-clave-segura

Cualquier solicitud de acceso al área en donde se encuentras alojados los servidores de la entidad, deberán ser previamente aprobado por el líder del área de sistemas, y las visitas deberán en acompañamiento de funcionarios encargados.

El mantenimiento de redes eléctricas, de voz y datos deberá ser realizada por personal idóneo apropiadamente autorizado e identificado.

Los ingresos a los centros de cableado en horarios no laborales deberán ser registrados, y cumplir completamente con los controles físicos establecidos.

Los funcionarios deberán portar el carnet que los identifique en un lugar visible mientras se encuentren en las instalaciones de la ESE Santiago de Tunja, en caso de pérdida del carnet, este deberá ser reportado de manera inmediata al área encargada.

### 6.6. Software utilizado

todo software que se adquiera para apoyo de los procesos de la entidad deberá ser adquirido de acuerdo a la normatividad vigente y cumplir con todos los lineamientos establecidos para para la adquisición según el manual de contratación.

Todas las instalaciones de software que sean requerida deberán ser previamente aprobadas por el líder del área de sistemas, evitando así que terceros puedan realizar instalaciones no permitida, cualquier software ilegal que sea instalado en los equipos de la entidad sin autorización previa será automáticamente desinstalado y ser reportado como un incidente de seguridad para realizar la respectiva investigación.

La instalación de software en los equipos deberá estar controlada mediante configuración, la cual solicitará usuario y contraseña de administrador al momento de realizar la instalación.

Las claves de administrador de los diferentes sistemas deben ser conservadas por el líder del área de sistemas y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Adicionalmente se debe elaborar, mantener y actualizar el procedimiento para la correcta definición, uso y complejidad de las claves de usuario.

Garantizar que dentro de la entidad exista una cultura informática que garantice el conocimiento por parte de usuarios, contratistas y practicantes de los riesgos que conlleva la instalación de software ilegal y las sanciones que esta acarrea según la legislación colombiana en los artículos 270, 271 y 272 de la Ley 599 de 2000 (Código Penal).

### 6.7. Actualización de hardware

Para el cambio de cualquiera de los componentes de los equipos de cómputo como memoria, procesadores, discos duros entre otros, deberá ser previamente realizada una evaluación técnica autorizada por las áreas de sistemas.

Cualquier reparación actualización o mejora de los equipos que requiera la apertura, únicamente deberá ser realizada por el personal técnico a cargo y proceso deberá ser documentado cuando exista garantía vigente cunado no exista una garantía de los componentes a reemplazar.

Los equipos, impresoras, scanner, cables de red, modem. Switch, servidores o cualquier otro componente de las redes de comunicación no deberá ser reubicado sin la previa aprobación de las personas de sistemas.

### 6.8. Almacenamiento y respaldo

El Líder de Sistemas, determina el cronograma de actividades para la obtención de copias de seguridad, diligenciando el formato de “Elaboración de Backup de la información” en el cual se indica: código, Fecha del Backup, Nombre del Archivo

del Backup, Extensión, Frecuencia del Backup, Backup Manual o Automático, Responsable de la Realización del Backup, Entregado a, Lugar donde reposa el Backup o lugar físico (DVD, disco duro extraíble, USB, etc.) y Observaciones.

Ambiente Producción: para este ambiente se definen los siguientes tipos de Backups:

- Full Backup: se realiza diariamente a las 12:30 a.m.
- Diferencial: se realiza cada hora a partir de las 3 a.m. hasta las 5 p.m.
- Log de Transacciones: se realizará cada 30 minutos.

Dependiendo de la criticidad de cada base de datos, se define los tipos de Backups que se implementarán para cada una de ellas. Para la retención de los Backups del ambiente de producción se tendrá en cuenta lo siguiente:

Backup diarios: Los Backups se alojará diariamente en una en la siguiente ruta del servidor: C:\BK-CNT\BACKUP el cual tendrá una retención de 24 horas. Posteriormente se lleva a un disco duro externo y tendrá una retención de 60 días.

Para efectos de las seguridades del software Enterprise se generará 2 copias de seguridad automática de las bases de datos del software Enterprise, cada 2 horas la cual se encuentra en la ruta del equipo servidor de laboratorio: D:\BACKUP ENTERPRISE\BACKUPS.bak y otra diaria la cual se encuentra en la siguiente ruta: D:\BACKUP ENTERPRISE\BACKUPS_DIARIO.bak, la cual se genera todos los días de manera automática a las nueve de la mañana Posteriormente se lleva a un disco duro externo y tendrá una retención de 60 días.

Una copia en la oficina y otra fuera de la empresa y se identificarán de la siguiente forma:

COPIA DE SEGURIDAD
ESE SANTIAGO DE TUNJA

| | |
|---|---|
| CODIGO DE COPIA: | |
| AREA O GRUPO FUNCIONAL: | |
| FECHA DE LA COPIA: | |
| NUMERO DE CARPETAS COPIADAS: | |
| NOMBRE RESPONSABLE: | |

El nombre del archivo de la copia de seguridad debe estar estructurado de La siguiente manera:

Las iniciales de la dependencia o Grupo Funcional, según tabl

| Dependencia o Grupo Funcional | Iniciales |
|---|---|
| SISTEMAS | SIST |
| MANTENIMIENTO | MANT |

las iniciales del software al que se le realiza la COPIA:

| Software | Iniciales |
|---|---|
| CNT | CNT |
| ENTERPRISE | ENT |

Periodo y año al que corresponde la copia, hora y tipo de archivo

Por ejemplo: SistCNT022820181714.bak

En donde SIST corresponde a la dependencia sistemas CNT software al cual se le realizo la copia en este caso CNT, 02 al mes de febrero, 28 día, 2018 año, 1714 corresponde a las 05:14 pm (hora) y .bak la extensión del archivo (esto puede variar según como se realice la copia de seguridad).

Backup mensual: Los Backups mensuales se alojarán en una carpeta compartida la cual es pasada a un disco duro externo y tendrá una retención de 12 meses.

Backup anual: se genera el último día del año y se lleva a disco duro externo y su retención será perpetua.

**COPIAS DE SEGURIDAD EQUIPOS USUARIOS**

El funcionario designado o responsable de la labor, ejecuta el proceso para la obtención de copias de seguridad, previo aviso al responsable del equipo; proceso que se realizará cada tres (3) meses a los equipos de los usuarios de la empresa.
En desarrollo de este proceso debe preguntar al responsable del equipo si se ha efectuado modificación al mapa de librerías o carpetas, y en caso afirmativo solicita copia de la misma; esta situación se registra en el formato de realización del proceso.
Las copias de seguridad se almacenan en el medio magnético previsto. Este dispositivo será rotulado y registrado su número de consecutivo o código, tal como se describió en el aparte anterior, en la planilla respectiva.

Los dispositivos de almacenamiento de las copias de seguridad, los entrega al Líder del Grupo Funcional de Sistemas, junto con la planilla de registro de los dispositivos.

Estos dispositivos junto con el original de la planilla relación de copias de seguridad, se depositan en sobre lacrado y rotulado para ser entregado como valor en custodia. De esta operación se efectuará el registro contable en cuentas fuera de balance, según las normas contables generalmente aceptadas; y se deja registro de esta operación.

**RESTAURACION DE LA INFORMACIÓN**.

El funcionario que desee consultar o restaurar alguna copia de seguridad, solicita al funcionario responsable del área de sistemas la recuperación de la información, indicando la fecha en la cual se realizó la copia.
El responsable del área de sistemas o el funcionario responsable de mantenimiento recupera la información solicitada en el DVD o USB de la copia de seguridad, para su respectiva consulta.

### 6.9. Soporte técnico

Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad la entidad, el usuario responsable debe informar a el área de mantenimiento para se pueda realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos dela entidad, solo puede ser realizado por el área de mantenimiento de la entidad, evitando así cualquier otro tipo de daño que realice por la inadecuada manipulación de los componentes.

Los equipos de cómputo deberán ser trasportados con las medidas se seguida apropiadas para garantizar la integridad física de los componentes.

### 6.10. Protección contra virus

### 6.11. Hardware

Un equipo de cómputo será asignado a cada funcionario para realizar sus actividades, cada equipo está dotado tanto de hardware como software de acuerdo con las necesidades de cada proceso, el usuario asignado al equipo no deberá alterar el contenido físico y lógico incluyendo todos sus periféricos. En caso de que el equipo asignado presente alguna falla se deberá notificar al área encargada para que se puedan realizar el diagnóstico y la reparación si es el caso, no intente reparar equipos impresores o cualquier otro dispositivo ya que esto podrá alterar el funcionamiento de los equipos y generar daños que comprometan otros componentes.

Cada usuario es responsable de su equipo y solo será utilizado para tareas asignadas a su cargo, de ninguna manera deberá ser utilizado para fines personales y abstenerse de realizar instalaciones de software no permitido por la entidad como software de entretenimiento o de terceros , de ser requerida la instalación de algún tipo de software no contemplado dentro de los permitido , deberás ser solicitado al áreas encargada para

que este pueda inicialmente realizar una evaluación y posteriormente ser instalada en la estación de trabajo de quien lo solicite , en caso de que el tipo de software sea de pago o requiera el pago de algún tipo de suscripción o licencimeinetro adicional , la adquisición será realizada por el área de sistemas .

### 6.12. correo electrónico

Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso al buzón asignado a cada funcionario de la entidad

Es una falta grave facilitar y ofrecer su cuenta de correo electrónico (e-mail) a personas no autorizadas, su cuenta es exclusiva del cargo o dependencia y no es transferible. De llegar a presentarse este tipo de situaciones el área de sistemas procederá a bloquear la cuenta por seguridad.

El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información masiva tipo spam o cadenas.

Están completamente prohibidas las siguientes actividades:

- Utilizar el Correo Electrónico para cualquier propósito comercial o financiero.
- No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la respectiva entidad.
- Enviar correo electrónico que contenga amenazas o mensajes violentos.
- utilizar la cuenta de correo electrónico institucional, en redes sociales como Facebook, Instagram u otro tipo de red que envié notificaciones o información al buzón que no tiene nada que ver con la entidad.

- Crear o intercambiar mensajes ofensivos u obscenos de cualquier clase, incluyendo material pornográfico
- Creación, reenvió o intercambio de mensajes SPAM (correo no solicitado), cadenas de cartas, solicitudes o publicidad.
- Crear, almacenar o intercambiar mensajes que contengan material protegido bajo las leyes de derechos de autor, sin el consentimiento de su(s) autor(es).
- Divulgar mensajes con datos o información institucional no autorizada.
- Divulgar sus contraseñas de correo.
- Alterar el contenido del mensaje de otro usuario sin su consentimiento.
- Utilizar como propia la cuenta de correo de otro funcionario sin su permiso.
- Inscribir la cuenta de correo en listas no relacionadas con la gestión de la entidad.
- borrar mensajes cuyo contenido es relevante o importante, dentro de las funciones asignadas como funcionario o para la entidad.
- Enviar mensajes con archivos anexos extensos, que puedan afectar el desempeño del servicio y de la red local.

La administración de las cuentas de correo electrónico es exclusiva de la dependencia de sistemas.

El Password o clave que se establece es generado automáticamente, se recomienda cambiarlo la primera vez que acceda a la plataforma de correo electrónico

No se pueden enviar archivos adjuntos con extensión ejecutable por lo cual no debería sorprender que se genere un mensaje automático de advertencia indicando el tema.

A través de la cuenta de correo se puede tramitar todo tipo de datos adjuntos, siempre y cuando el tamaño total del archivo no exceda de 25MB, ya sea para correos de entrada como de salida.

En caso de necesitar creación, reinicio o cancelación de la cuenta, así como cambio de la clave de acceso al correo, se deberá solicitar al área de sistemas para realizar el debido tramite.

## 7. VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD

A continuación son nombradas algunas de las actividades que son consideradas como violaciones a las políticas de seguridad:

- Enviar correos electrónicos no solicitado por los usuarios o contenido de tipo Spam.
- Envío de correo con contenidos pornográficos , bélicos , armas drogas o cualquier otro materia que afecte la buena moral de las personas.
- Instalación o ejecución de software malintencionado sin autorización autorizado.
- Utilización del internet indebidamente, esto incluye, navegación a páginas con contenidos pornográficos, sitios de música en línea, juegos en línea, sistemas de mensajería instantánea (no autorizados), casinos, proxys piratas, programas de carga de archivos, o cualquier otro sitio con fines diferentes a los laborales.
- Traslado, manipulación o instalación de nuevos equipos a la red sin la autorización ni el procedimiento establecido por el proceso de recursos tecnológicos.
- Dañar física o lógicamente los equipos o la infraestructura informática.

- Instalar dispositivos o tarjetas de acceso remoto, módems. RDSI, ROUTERS o cualquier otro dispositivo de comunicaciones en los clientes de la red.
- Utilizar cualquiera de los recursos informáticos de la ese Santiago de Tunja para fines diferentes a las funciones contractuales, ya sea funcionario o contratista.
- Utilizar cualquier tipo de software para fines malicioso o intrusos tales como SNIFFERS, scanner, KEYLOGGERS, entre otros.
- Utilizar cualquier técnica de hacking hacia cualquiera de los recursos tecnológicos de la entidad entre los que se incluye, ataques DOS, PHISING, SPOOFING y BROADCAST.

## 8. TRATAMIENTOS DE DATOS PERSONALES

La Ese Santiago de Tunja dentro de sus manuales tiene el tratamiento de datos personales en atención al objeto determinado por la Ley 1581 de 2012: "*La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.*"

"*Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.*"