Empresa Social del Estado
Santiago de Tunja

E.S.E SANTIAGO DE TUNJA

MANUAL 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 video online, 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]

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

El sistema de información dinámica gerencial, se encuentra avalado y certificado según notificación emitida por la casa desarrolladora sistemas y asesorías de Colombia S.A (SYAC):

SYAC
www.syac.net.co

DINAMICA GERENCIAL

Bogotá, 30 De Abril de 2021

Señores
E.S.E SANTIAGO DE TUNJA
Boyacá

CERTIFICACION

SISTEMAS Y ASESORÍAS DE COLOMBIA S.A. (SYAC) certifica que el manejo que el sistema Dinámica Gerencial de los módulos licenciados a la ESE cumple con lo estipulado por la normatividad Colombiana y de igual forma el Sistema garantiza que la Información almacenada, procesada y generada cumple con los atributos de inalterabilidad, integridad, seguridad y conservación, en lo que respecta al software en sí mismo considerado y desde la idoneidad y calidad del producto, que el fabricante está en posibilidad de acreditar.

Sin perjuicio de ello, el contratista es ajeno a casos de fuerza mayor, casos fortuitos y hechos de terceros, ajenos a su competencia y diligencia que eventualmente impidan garantizar de manera absoluta la inalterabilidad, integridad y seguridad de la información.

El diligenciamiento y la veracidad de los datos de la información registrada, serán responsabilidad única y exclusiva de la ESE SANTIAGO DE TUNJA , de conformidad con las normas que regulan la materia.

Dinámica Gerencial genera información por medios como pantallas, impresiones físicas o archivos magnéticos. Es responsabilidad del comerciante y/o Contratante la manipulación que realice sobre la información proporcionada por DGH en los medios mencionados que genere cambios que pueden alterar y ocasionar la perdida de integridad.

Cordialmente,

PEDRO FELIPE CERON Y CERON
Gerente Comercial – SYAC

CMMIDEV/5

PBX: (1)756-0520 Av. Cra. 45 No. 108 - 27 | Torre 2 - Of. 1405 | Bogotá - Colombia
www.syac.net.co

SYAC

DINAMICA GERENCIAL
La diferencia entre tener la información y hacer buen uso de ella

Bogotá, D.C., 16 de diciembre del 2022

EMPRESA SOCIAL DEL ESTADO
SANTIAGO DE TUNJA
RECIBIDO
Fecha 19 DIC. 2022
Hora: 08:56 No. 6700
Recibio Martha Parra

Señores:
E.S.E. SANTIAGO DE TUNJA
Ing. **William Ricardo Mateus Burbano**
Supervisor contrato
Tunja - Boyacá

Cordial Saludo Ing. Mateus,

Atentamente me permito remitir la siguiente documentación para su trámite correspondiente:

- Certificación original de licencia debidamente firmada
- Dos (2) Licencias de uso No. 449 originales debidamente firmadas

Agradecemos hacer devolución de una licencia de uso original No. 449 debidamente firmada por parte de ustedes para que repose en nuestro archivo.

Gracias.

Cordialmente,

MISHELL GÓMEZ CÁRDENAS
Asistente de Comercial

SYAC S.A.

CERTIFICA:

SISTEMAS Y ASESORIAS DE COLOMBIA S.A. - SYAC en su calidad de único titular de los derechos de licenciamiento del software "**DINAMICA GERENCIAL**", certifica que la **E.S.E SANTIAGO DE TUNJA** identificada con numero de NIT: **820.003.850 - 2** tiene licenciados los siguientes módulos del programa:

Módulo		Módulo	
ACTIVOS FIJOS .NET	X	ADMISIONES .NET	X
CARTERA .NET	X	CITAS MEDICAS .NET	X
COMPRAS .NET	X	CONTRATOS IPS .NET	X
COSTOS HOSPITALARIOS .NET	X	FACTURACION .NET	X
GENERALES & SEGURIDAD .NET	X	GESTION GERENCIAL .NET	X
HISTORIAS CLINICAS .NET	X	HOSPITALIZACION .NET	X
INFORMACION FINANCIERA NIIF .NET	X	INVENTARIOS .NET	X
LABORATORIO .NET	X	NOMINA .NET	X
PAGOS .NET	X	PRESUPUESTO .NET	X
PROMOCION Y PREVENCION .NET	X	TESORERIA .NET	X
WEB CITAS MEDICAS	X	WEB HISTORIAS CLINICAS .NET	X

La anterior información puede ser validada en la licencia de uso No. **449** la cual se adjunta al presente documento.

Cordialmente,

ALVARO AUGUSTO CANO HERNANDEZ
REPRESENTANTE LEGAL
SYAC S.A.

LICENCIA DE USO DEL PROGRAMA DE SOFTWARE: "DINÁMICA GERENCIAL"	No. CONSECUTIVO 449

LICENCIANTE:	Sistemas y Asesorías de Colombia S.A. - SYAC
NIT:	800.149.562-0
Domicilio:	Av. Cra. 45 No. 108 - 27 Torre 2 - Of. 1408 Bogotá - Colombia
LICENCIATARIO:	E.S.E. SANTIAGO DE TUNJA
NIT:	NIT: 820003850 - 2
Domicilio:	Calle 16 No. 11-19

El presente documento contiene la Licencia de uso del software "DINÁMICA GERENCIAL".

I. El Licenciante Sistemas y Asesorías de Colombia S.A. - SYAC tiene la calidad de parte productor de la obra: "DINÁMICA GERENCIAL" (tal conforme consta en el correspondiente Certificado de Registro de Soporte Lógico, expedido por la Dirección Nacional de Derechos de Autor, del Ministerio del Interior y de Justicia), y se encuentra legitimado para ejercer los derechos de explotación económica de la obra en comento, incluyendo su comercialización y su distribución así como de todos los y productos conexos y complementarios derivados de la misma; por tiempo indefinido y en exclusiva, para todo el ámbito territorial mundial.

II. Al Licenciatario se le otorga la presente licencia de uso del software DINÁMICA GERENCIAL, de conformidad con el contrato de licenciamiento suscrito entre las partes

III. Sobre la base de lo anterior, el Licenciante y el Licenciatario aceptan los términos y condiciones que se encuentran como anexo a la propuesta economica aprobada o contrato de licenciamiento suscrito entre las partes, que han de regir la licencia de uso del software DINÁMICA GERENCIAL.

IV. Sistemas y Asesorías de Colombia S.A. - SYAC en su calidad de único titular de los derechos de licenciamiento del software "DINAMICA GERENCIAL", concede el uso de una (1) licencia de uso de los siguientes módulos del programa:

Módulo		Módulo	
ACTIVOS FIJOS .NET	X	ADMISIONES .NET	X
CARTERA .NET	X	CITAS MEDICAS .NET	X
COMPRAS .NET	X	CONTRATOS IPS .NET	X
COSTOS HOSPITALARIOS .NET	X	FACTURACIÓN .NET	X
GENERALES & SEGURIDAD .NET	X	GESTION GERENCIAL .NET	X
HISTORIAS CLINICAS .NET	X	HOSPITALIZACIÓN .NET	X
INFORMACIÓN FINANCIERA NIIF .NET	X	INVENTARIOS .NET	X
LABORATORIO .NET	X	NOMINA .NET	X
PAGOS .NET	X	PRESUPUESTO .NET	X
PROMOCION Y PREVENCION .NET	X	TESORERIA .NET	X
WEB CITAS MEDICAS	X	WEB HISTORIAS CLINICAS	X

V. Vigencia / Licencia Permanente: Cuando el Licenciatario haya adquirido una licencia permanente adquiere el derecho de uso del programa / software sin limite en el tiempo, en la versión que se indica en el contrato de licenciamiento respectivo, sin que ello implique el derecho a usar actualizaciones o nuevas versiones del software salvo las previstas en ese contrato

VI. Aceptación del producto: Una vez entregado este documento total y correctamente diligenciado a Sistemas y Asesorías de Colombia S.A. - SYAC, quedará oficialmente registrada una (1) licencia de uso en favor del Licenciatario.

ACEPTACIÓN:

FIRMA DEL REPRESENTANTE LEGAL Y SELLO DEL LICENCIANTE	FIRMA DEL REPRESENTANTE LEGAL Y SELLO DEL LICENCIATARIO
Nombre: Alvaro Augusto Cano Hernandez	Nombre:
Cargo: Representante legal	Cargo:
NIT: 800149562-0	NIT:

La cual garantiza la correcta oración de las actividades.

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.

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

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 seis (6) meses a los equipos de los usuarios de la empresa seccional administrativa según cronograma socializado con los líderes de proceso. 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 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 licenciamiento 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 trámite.

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.*"

CONSIDERANDO:

La Empresa Social del Estado Santiago de Tunja fue creada por medio del Acuerdo Municipal No. 007 del 03 de febrero de 1999, modificada por el Acuerdo Municipal No. 011 del 6 de mayo de 2002, con categoría especial de entidad pública descentralizada del orden municipal, dotada de personería jurídica, patrimonio propio y autonomía administrativa; adscrita a la Secretaría de salud e integrante del Sistema General de Seguridad Social en Salud y sometida al régimen jurídico previsto en el capítulo III, Artículo 194 y 195 de la Ley 100 de 1993.

Que el modelo integrado de Planeación y Gestión MIPG, busca mejorar la capacidad del estado para cumplirle a los grupos de valor, incrementando la confianza de estos en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna.

En Colombia, la normativa principal que garantiza el tratamiento adecuado de datos personales es la Ley Estatutaria 1581 de 2012, conocida como la Ley de Protección de Datos Personales. Esta ley establece los principios, derechos y obligaciones relacionados con la protección de datos personales y regula su recolección, almacenamiento, uso, circulación y supresión.

La Ley 1581 de 2012 establece los siguientes aspectos clave para el tratamiento de datos personales:

1. Consentimiento informado: La ley establece que el tratamiento de datos personales requiere el consentimiento previo, expreso e informado de la persona titular de los

datos. Además, se establecen requisitos específicos para obtener el consentimiento, como informar al titular sobre la finalidad del tratamiento y los derechos que le asisten.

2. Principios de protección de datos: La ley establece los principios que deben regir el tratamiento de datos personales, incluyendo el principio de finalidad, necesidad, libertad, veracidad, transparencia, seguridad y confidencialidad.
3. Derechos de los titulares de los datos: La normativa garantiza los derechos de los titulares de los datos, como el derecho de acceso, rectificación, actualización, supresión y oposición al tratamiento de sus datos personales. También se establece el derecho a presentar reclamaciones ante la autoridad de protección de datos en caso de violación de sus derechos.
4. Medidas de seguridad: La ley exige a las entidades que realicen el tratamiento de datos personales implementar medidas técnicas, administrativas y humanas necesarias para garantizar la seguridad de los datos y prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado.

Además de la Ley 1581 de 2012, existen otras normativas y decretos complementarios en Colombia que regulan aspectos específicos del tratamiento de datos personales, como el Decreto 1377 de 2013, Resolución 078 del 17 de Abril de 2017, por medio de la cual se deroga la resolución 043 del 28 de Febrero del 2014 y se establece la política de tratamiento y protección de los datos personales establecen un marco legal en Colombia que garantiza la protección de datos personales y regula su tratamiento, con el objetivo de preservar la privacidad y seguridad de los ciudadanos y fomentar un uso responsable de la información personal.

En este sentido la política de tratamiento de datos personales de la Empresa Social del Estado Santiago de Tunja tendrá como propósito fundamental establecer los lineamientos y principios que guiarán el manejo adecuado de la información personal por parte de una organización. Esta política tiene como objetivo principal garantizar la protección de los derechos de los titulares de los datos y asegurar el cumplimiento de las normativas y regulaciones aplicables en materia de protección de datos.

La política de tratamiento de datos personales busca promover la transparencia y la confianza en la gestión de la información personal, tanto de clientes, empleados, proveedores u otras partes interesadas. A través de esta política, se definen los procedimientos, responsabilidades y medidas de seguridad que se deben implementar para salvaguardar la privacidad y confidencialidad de los datos personales.

Además, la política de tratamiento de datos personales establece los derechos y deberes de las partes involucradas en el proceso de tratamiento de datos, incluyendo los derechos de los titulares de la información para acceder, rectificar, actualizar y suprimir sus datos, así como la obligación de la organización de obtener autorización previa para el tratamiento de los datos personales.

La política también tiene como propósito promover una cultura de protección de datos dentro de la organización, a través de la sensibilización, capacitación y supervisión de los empleados y colaboradores en cuanto a las buenas prácticas en el manejo de la información personal.

En resumen, el propósito fundamental de la Política de Tratamiento de Datos Personales es establecer un marco normativo y operativo que permita a la organización gestionar de manera responsable y ética los datos personales, garantizando la privacidad, seguridad y confidencialidad de la información, así como el respeto a los derechos de los titulares de los datos.

Por lo anteriormente expuesto y dando cumplimiento de este mandato el Gerente de la Empresa Social Del Estado Santiago De Tunja:

RESUELVE

ARTICULO PRIMERO Adóptese la Política De Tratamiento De Datos de la E.S.E Santiago de Tunja.

1. POLITICA TRATAMIENTO DE DATOS PERSONALES

En la era de la información en la que vivimos, el tratamiento de datos personales se ha convertido en un aspecto crítico de nuestra vida digital. A medida que avanzamos hacia una sociedad cada vez más conectada, la cantidad de datos personales generados, compartidos y almacenados ha alcanzado niveles sin precedentes. Esta creciente cantidad de información plantea desafíos significativos en términos de privacidad y seguridad. El tratamiento adecuado de los datos personales se vuelve esencial para salvaguardar nuestra identidad, proteger nuestra privacidad y mantener la confianza en la era digital.

Los datos personales abarcan una amplia gama de información, que incluye nombres, direcciones, números de teléfono, direcciones de correo electrónico, información financiera

y de salud, preferencias personales y mucho más. Estos datos, en manos equivocadas, pueden dar lugar a consecuencias graves, como el robo de identidad, el fraude financiero y la invasión de la privacidad.

Es por eso que el tratamiento adecuado de los datos personales se ha convertido en un imperativo para garantizar la protección de la información sensible y mantener la integridad de nuestra identidad en línea; El tratamiento adecuado de los datos personales implica una serie de medidas y prácticas diseñadas para garantizar su seguridad y privacidad. Esto implica la adopción de políticas claras y transparentes sobre la recopilación, el uso y la retención de datos personales, así como la implementación de medidas técnicas y organizativas para protegerlos de accesos no autorizados, divulgación no deseada o uso indebido. Además, el tratamiento adecuado implica respetar los derechos de los individuos, como el derecho a acceder, corregir o eliminar sus datos personales, y obtener su consentimiento informado antes de utilizar su información para fines específicos.

En resumen, el tratamiento adecuado de los datos personales se ha vuelto crucial en la sociedad digital actual. Proteger la privacidad, garantizar la seguridad y cumplir con las regulaciones de protección de datos son aspectos fundamentales para mantener la confianza y salvaguardar nuestra identidad en línea. Tanto los individuos como las organizaciones tienen la responsabilidad de adoptar medidas adecuadas de tratamiento de datos para construir una sociedad digital segura y confiable.

2. ALCANCE DE LA POLITICA

El alcance de una política de tratamiento y protección de datos personales en la E.S.E Santiago de Tunja se centra en garantizar la privacidad, seguridad y confidencialidad de la información médica y personal de los pacientes. Esta política se basa en la Ley Estatutaria 1581 de 2012 y otras normativas relacionadas, así como en los principios éticos y deontológicos propios de la práctica médica.

3. OBJETIVOS

- Garantizar el cumplimiento de las leyes y regulaciones aplicables: Uno de los principales objetivos de una política de tratamiento y protección de datos personales es asegurar que la organización cumpla con las leyes y regulaciones vigentes en materia de protección de datos. Esto implica establecer los procedimientos y controles necesarios para garantizar el cumplimiento de las normativas, evitando posibles sanciones legales y daños a la reputación de la organización.
- Proteger la privacidad y confidencialidad de los datos personales: La política busca salvaguardar la privacidad y confidencialidad de la información personal que la organización maneja. Esto implica establecer medidas de seguridad adecuadas para prevenir el acceso no autorizado, la divulgación o pérdida de datos, así como asegurar su integridad y disponibilidad. El objetivo es proteger los datos personales de los titulares y evitar su uso indebido o fraudulentos.
- Establecer roles y responsabilidades claras: Una política efectiva define los roles y responsabilidades de los diferentes actores involucrados en el tratamiento de datos

personales, tanto a nivel gerencial como a nivel operativo. Esto incluye designar a un encargado o responsable de protección de datos, así como asegurar que todos los empleados estén conscientes de sus responsabilidades en la protección de la información personal.

- Promover la transparencia y confianza: La política busca fomentar la transparencia en el manejo de datos personales, informando a los titulares sobre cómo se recopilan, utilizan y protegen sus datos. Esto incluye proporcionar información clara y comprensible sobre las finalidades del tratamiento, los derechos de los titulares y los procedimientos para ejercer dichos derechos. El objetivo es generar confianza en los titulares de los datos y fortalecer la relación de la organización con sus clientes, empleados y otras partes interesadas.
- Establecer mecanismos de respuesta y atención a solicitudes y reclamos: La política debe incluir procedimientos claros y eficientes para tramitar y responder las solicitudes y reclamos relacionados con el tratamiento de datos personales. Esto implica establecer canales de comunicación y plazos de respuesta, así como capacitar al personal encargado de atender estas solicitudes. El objetivo es garantizar que los titulares puedan ejercer sus derechos y recibir una respuesta oportuna y adecuada por parte de la organización.

4. LINEAS DE ACCIÓN

- Gestión de riesgos y seguridad de la información: Una línea de acción importante en la política de tratamiento de datos personales es establecer medidas de gestión de riesgos y seguridad de la información. Esto implica identificar y evaluar los riesgos asociados al manejo de datos personales, implementar controles y medidas

de seguridad apropiadas para mitigar dichos riesgos, y realizar seguimiento y monitoreo continuo para garantizar la protección de la información.

- Capacitación y concientización: Es fundamental contar con una línea de acción que promueva la capacitación y concientización de todos los empleados y colaboradores sobre las políticas y procedimientos de tratamiento de datos personales. Esto incluye la formación en las leyes y regulaciones aplicables, las mejores prácticas de privacidad y protección de datos, así como la importancia de cumplir con las políticas internas de la organización. La capacitación continua ayudará a garantizar que todos los miembros de la organización estén alineados y comprometidos con la protección de los datos personales.
- Auditoría y monitoreo: Otra línea de acción relevante es la implementación de mecanismos de auditoría y monitoreo para asegurar el cumplimiento de la Política de Tratamiento de Datos Personales. Esto implica realizar auditorías periódicas para evaluar la conformidad con las políticas y procedimientos establecidos, así como llevar a cabo un monitoreo continuo de las actividades de tratamiento de datos para identificar posibles incumplimientos o vulnerabilidades. Los resultados de estas auditorías y monitoreos ayudarán a identificar áreas de mejora y tomar acciones correctivas necesarias.

5. IMPLEMENTACIÓN DE ESTRATEGIAS

Autorización para el Tratamiento de Datos Personales

La autorización del titular de la información debe ser suministrada de forma expresa y de manera previa al tratamiento; toda vez que el titular debe estar plenamente informado de los efectos de su autorización.

Con el fin de garantizar lo mencionado anteriormente, se establecerá un procedimiento para obtener la autorización necesaria del titular de los datos personales al incorporar su información en las bases de datos de la E.S.E Santiago de Tunja, procedimiento consistirá en proporcionar al titular un documento de autorización para el tratamiento de datos personales, ya sea en formato físico o electrónico.

El documento de autorización deberá incluir, como mínimo, información sobre el tipo de tratamiento al que serán sometidos los datos personales y la finalidad del mismo. En el caso de no contar con la autorización previa y expresa del titular, los Servicios de Salud se abstendrán de realizar cualquier tratamiento de dicha información.

Sin embargo, existen situaciones específicas en las cuales no será necesario obtener la autorización del titular para llevar a cabo el tratamiento de sus datos. Estos casos excepcionales deberán ser previamente establecidos y justificados en la política de tratamiento de datos personales de los Servicios de Salud.

Es importante destacar que esta política de autorización busca asegurar el cumplimiento de las regulaciones y normativas de protección de datos, así como garantizar la privacidad y seguridad de la información personal de los titulares. Al obtener la autorización previa y expresa, los Servicios de Salud demuestran su compromiso con el respeto a los derechos de privacidad y protección de datos de los individuos, promoviendo una relación

transparente y confiable con sus usuarios, con excepción de los siguientes eventos en los cuales no será necesaria la autorización:

- Llevar a cabo medidas necesarias para la ejecución de un contrato que se haya celebrado con el titular.
- Enviar información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Realizar tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Realizar tratamiento de datos de naturaleza pública, o aquellos relacionados con el registro civil de las personas.

Tratamiento y Finalidades

En el contexto de la E.S.E. Santiago de Tunja, se reconoce la importancia de los datos personales y se establecen las finalidades generales para su tratamiento. Estas finalidades abarcan acciones como la recolección, recaudación, transferencia, almacenamiento, uso, circulación, supresión, procesamiento, compartición, actualización, intercambio y disposición de los datos personales.

Es fundamental destacar que estas acciones se llevarán a cabo con estricto cumplimiento de las regulaciones y normativas de protección de datos vigentes, y siempre respetando los derechos de privacidad y protección de los titulares de los datos.

Algunas de las finalidades generales establecidas para el tratamiento de los datos personales en la E.S.E. Santiago de Tunja son:

- Brindar servicios de atención médica y cuidado de la salud a los pacientes, asegurando un adecuado seguimiento y tratamiento de sus condiciones médicas.
- Administrar y gestionar la información necesaria para el funcionamiento eficiente de la institución, incluyendo aspectos administrativos, financieros y logísticos.
- Realizar investigaciones científicas y estudios epidemiológicos con el fin de mejorar la calidad de la atención médica y contribuir al avance del conocimiento en el ámbito de la salud.
- Cumplir con obligaciones legales y regulatorias establecidas por las autoridades competentes, incluyendo la facturación, el reporte de información estadística y la implementación de medidas de seguridad y prevención de riesgos.
- Garantizar la seguridad y protección de los datos personales, implementando medidas técnicas y organizativas adecuadas para prevenir el acceso no autorizado, la pérdida, alteración o divulgación indebida de la información.

Es importante mencionar que estas finalidades generales deben estar respaldadas por una política de tratamiento de datos personales que establezca los procedimientos y medidas necesarios para garantizar el cumplimiento de la normativa de protección de datos, así como los derechos de los titulares de los datos.

- Prestación de servicios asistenciales a pacientes y sus familias.
- Gestión administrativa de la atención en salud.

- Comunicación de información relevante sobre servicios de salud, actividades, eventos académicos y empresariales, publicaciones, publicidad relacionada con la salud, boletines de prensa, innovación empresarial, mensajes de protocolo, tarjetas de Navidad e informes de gestión.
- Promoción de otros canales digitales, como sitios web, blogs, redes sociales y videos relacionados con la E.S.E. Santiago de Tunja "Calidad para la vida".
- Cumplimiento de obligaciones legales y requisitos impuestos por entidades reguladoras y supervisores del sector salud, así como otras autoridades competentes.
- Cumplimiento de obligaciones derivadas de relaciones contractuales y comerciales existentes.
- Identificación prospectiva de las necesidades de los grupos de interés con el objetivo de innovar en la prestación de servicios.
- Recopilación de datos a través de encuestas, formularios y evaluación de indicadores de oportunidad y calidad de los servicios.
- Utilización de datos para fines de investigación, ciencia, formación y educación.
- Mantenimiento de la seguridad de pacientes, colaboradores, visitantes, terceros y cualquier persona que ingrese a las instalaciones de la E.S.E. Santiago de Tunja.
- Mejora de la eficiencia, seguridad y tecnología en los procesos.
- Actualización de los datos proporcionados por el titular de los mismos.

Es importante destacar que todas estas actividades se llevarán a cabo cumpliendo con las leyes y regulaciones de protección de datos aplicables. La E.S.E. Santiago de Tunja

implementará las medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales durante su tratamiento.

Además de las finalidades generales, existen finalidades particulares relacionadas con la relación de los titulares de los datos personales con la organización, que se describen a continuación:

Finalidades especiales para el tratamiento de los datos de pacientes y sus familias:

- Obtener datos fundamentales para la investigación clínica y epidemiológica.
- Enviar resultados de exámenes diagnósticos.
- Comunicación relacionada con nuestros servicios a través de diversos medios.
- Informar sobre campañas, programas especiales, promoción de servicios y educación para el usuario.
- Realizar encuestas de satisfacción de servicios y atención prestada.
- Atender solicitudes de mejora, peticiones, quejas, sugerencias y reclamos, y realizar su seguimiento.
- Realizar caracterización y seguimiento de la población para gestionar el riesgo en salud, utilizando información derivada de los servicios asistenciales.

Finalidades especiales para el tratamiento de los datos personales de empleados:

- Publicaciones internas y externas.
- Acceso a plataformas tecnológicas propias de la organización.

- Compartir información con empresas que necesiten verificar datos laborales de los empleados.
- Comunicar jornadas de capacitación y programas de mejora continua.
- Informar sobre procesos de selección y promoción interna.
- Establecer y gestionar relaciones contractuales.
- Realizar evaluaciones de desempeño, satisfacción laboral, nómina, crecimiento personal, bienestar, seguridad y salud en el trabajo.
- Cumplir con el proceso de afiliación al Sistema General de Seguridad Social Integral.
- Emitir certificaciones laborales, como certificados de ingresos y retenciones, constancias laborales, entre otros.

Finalidades especiales para el tratamiento de los datos personales de proveedores, clientes, contratistas, convenios y alianzas:

- Evaluar bienes y servicios prestados por las partes.
- Realizar seguimiento y gestión de la relación contractual.
- Reportar reclamaciones a compañías aseguradoras cuando corresponda.
- Cumplir con las finalidades propias de la celebración, ejecución, evolución, terminación y liquidación de la relación contractual.

Es importante destacar que todas estas finalidades se llevarán a cabo cumpliendo con la normativa vigente en protección de datos y respetando los derechos de los titulares de los

datos. La E.S.E Santiago de Tunja implementará las medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales durante su tratamiento.

Derechos y Deberes

Derechos del Titular de Datos Personales

De acuerdo con lo establecido en el artículo 8 de la Ley 1581 de 2012, el titular de los datos personales cuenta con los siguientes derechos:

- Derecho de conocer, actualizar y rectificar sus datos personales.
- Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento de la información.
- Derecho a ser informado por la E.S.E. Santiago de Tunja, previa solicitud, acerca del uso que se les han dado a sus datos personales.
- Derecho a presentar quejas ante la Superintendencia de Industria y Comercio por posibles infracciones a lo establecido en la Ley 1581 de 2012, una vez se haya agotado el proceso de consulta o reclamo ante la E.S.E. Santiago de Tunja, en calidad de responsable del tratamiento.
- Derecho a revocar la autorización y/o solicitar la supresión de sus datos cuando el tratamiento no cumpla con los principios, derechos y garantías constitucionales y legales.
- Derecho de acceso gratuito a sus datos personales que hayan sido objeto de tratamiento.

Estos derechos son fundamentales para proteger la privacidad y control de los datos personales de los titulares. La E.S.E. Santiago de Tunja se compromete a respetar y garantizar el ejercicio de estos derechos, de acuerdo con las disposiciones legales

aplicables y las medidas de seguridad necesarias para salvaguardar la información personal.

Derechos de los Niños, Niñas y Adolescentes

En el contexto del tratamiento de datos personales llevado a cabo por la E.S.E. Santiago de Tunja, se garantiza el pleno respeto a los derechos prevalentes de los niños, niñas y adolescentes. Por lo tanto, se prohíbe terminantemente el tratamiento de datos personales de este grupo, a menos que los datos en cuestión sean de naturaleza pública y el tratamiento cumpla con los siguientes parámetros y requisitos:

- Que el tratamiento de datos responda y salvaguarde el interés superior de los niños, niñas y adolescentes. Esto implica que cualquier acción relacionada con la recolección, almacenamiento, uso y divulgación de sus datos personales debe tener como finalidad principal su beneficio y bienestar.
- Que se garantice el pleno respeto de los derechos fundamentales de los niños, niñas y adolescentes en el tratamiento de sus datos personales. Esto incluye, entre otros, el derecho a la privacidad, la integridad personal, la no discriminación y la participación activa en los procesos que afecten sus derechos.

Una vez cumplidos los requisitos mencionados anteriormente, la autorización para el tratamiento de los datos personales de un niño, niña o adolescente será otorgada por su representante legal. Sin embargo, es importante destacar que antes de tomar una decisión, se deberá garantizar el ejercicio de los derechos del menor a ser escuchado, a recibir información y a la libertad de expresión. La opinión del menor será tenida en cuenta, considerando su nivel de madurez, autonomía y capacidad para comprender el asunto en cuestión.

Este enfoque garantiza que el tratamiento de los datos personales de niños, niñas y adolescentes se realice de manera responsable, respetando plenamente sus derechos y considerando su capacidad de decisión de acuerdo con su desarrollo y etapa de vida. La E.S.E. Santiago de Tunja asume su compromiso de proteger la privacidad y los derechos de este grupo vulnerable, asegurando que cualquier actividad relacionada con sus datos personales esté orientada a su beneficio y protección.

Deberes del responsable y/o Encargado del Tratamiento

En los procesos organizacionales de la E.S.E. Santiago de Tunja, se reconoce plenamente que los datos personales son propiedad de las personas naturales a las que se refieren y que únicamente ellas tienen el derecho de decidir sobre su uso. En este sentido, la E.S.E. Santiago de Tunja solo utilizará los datos personales en aquellas finalidades para las cuales ha obtenido la autorización correspondiente, en cumplimiento de los mandatos constitucionales, la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Conforme a lo establecido en la normativa vigente, la E.S.E. Santiago de Tunja se compromete a cumplir de manera permanente con los deberes consagrados en el artículo 17 de la Ley 1581 de 2012, en relación con la protección de datos personales. Estos deberes son los siguientes:

- Garantizar al titular de los datos, en todo momento, el pleno y efectivo ejercicio del derecho de Habeas Data, el cual le permite conocer, actualizar, rectificar y suprimir su información personal, así como oponerse a su tratamiento.
- Solicitar y conservar una copia de la autorización otorgada por el titular de los datos, en la cual se especifica la finalidad del tratamiento.

- Informar de manera clara y completa al titular sobre la finalidad de la recolección de sus datos, así como los derechos que le asisten como consecuencia de la autorización otorgada.
- Conservar la información bajo condiciones de seguridad que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Esto implica implementar medidas técnicas, administrativas y físicas para proteger los datos personales.
- Garantizar que la información suministrada sea veraz, completa, exacta, actualizada, comprobable y comprensible. En caso de que existan cambios en los datos, la E.S.E. Santiago de Tunja deberá comunicar al titular dichas modificaciones y tomar las medidas necesarias para mantener la información actualizada.
- Rectificar la información cuando sea incorrecta y comunicar dicha corrección al titular de los datos.
- Suministrar al encargado del tratamiento únicamente aquellos datos que estén previamente autorizados por el titular.
- Exigir al encargado del tratamiento que respete en todo momento las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados por los titulares de los datos, asegurando una respuesta oportuna y adecuada.
- Adoptar un manual interno de políticas y procedimientos que garantice el cumplimiento adecuado de la ley y, en particular, establezca los mecanismos para atender consultas y reclamos relacionados con la protección de datos personales.

- Informar al titular, a solicitud de este, sobre el uso que se ha dado a sus datos personales.
- Notificar a la autoridad de protección de datos cualquier violación a los códigos de seguridad establecidos y los riesgos existentes en la administración de la información de los titulares.

El Ejercicio de los Derechos del Titular

Los titulares de la información podrán, en cualquier momento, ejercer los derechos consagrados en la Ley 1581 de 2012 de conocer, actualizar y rectificar sus datos personales, solicitar prueba de la autorización otorgada para el tratamiento, informarse sobre el uso que se ha dado a los datos, revocar la autorización y solicitar la supresión de sus datos cuando sea procedente.

Para el ejercicio de estos derechos, el titular de la información podrá acudir a los siguientes canales de comunicación de la E.S.E. Santiago de Tunja:

Documento escrito: Dirigido a la Oficina Jurídica, en la Calle 16 No 9 – 41 Tunja.

Email : notificacionesjudiciales@esesantiagodetunja.gov.co

El titular del dato y/o interesado en ejercer uno de estos derechos, acreditará esta condición mediante comunicación escrita (Física o digital), anexando copia de su documento de identidad. En caso de que el titular este representado por un tercero deberá allegarse el respectivo poder, el apoderado deberá igualmente acreditar su identidad en los términos indicados.

En la solicitud para ejercer su derecho de Habeas Data, se deberá suministrar con precisión y veracidad los datos de contacto (dirección física, teléfono, correo electrónico, etc.) para efectos de dar respuesta y atender su solicitud; indicando el nombre e

identificación del titular y de sus representantes, de ser el caso y la petición concreta y precisa de información, acceso, actualización, rectificación, cancelación, oposición al tratamiento y/o revocatoria del consentimiento.

La E.S.E. Santiago de Tunja documentará y almacenará las solicitudes realizadas por los titulares de los datos o por los interesados en ejercicio de cualquiera de los derechos, así como las respuestas a tales solicitudes.

Consultas de Dase de Datos

La Política de Tratamiento de Datos Personales de la E.S.E. Santiago de Tunja garantiza el derecho de los titulares de los datos a consultar la información personal almacenada en las bases de datos de la organización. La consulta puede realizarse a través de medios físicos o electrónicos designados para este propósito. La E.S.E. Santiago de Tunja se compromete a responder a las consultas en un plazo máximo de diez (10) días hábiles a partir de su recepción.

En caso de que no sea posible atender la consulta dentro de dicho plazo, se informará al interesado antes de que expire el plazo de los 10 días, explicando las razones del retraso y proporcionando una fecha límite de respuesta que no excederá los cinco (5) días hábiles posteriores. La E.S.E. Santiago de Tunja, como parte de su deber de información, advierte a las personas interesadas en registrarse en sus bases de datos y portal web que son responsables de suministrar datos personales veraces y confiables.

Se establece que el uso de datos personales que no sean propios por parte de terceros será responsabilidad de la persona que los utilice, y estará sujeta a las sanciones

establecidas por la legislación colombiana en caso de violación de datos personales. La E.S.E. Santiago de Tunja asume de buena fe que la información personal proporcionada por los titulares de los datos está actualizada, es exacta, veraz y confiable, eximiéndose así de cualquier responsabilidad en cuanto a la calidad de dicha información.

Disposiciones de seguridad

Con el objetivo de proteger los datos personales, la E.S.E. Santiago de Tunja aplicará rigurosas medidas de seguridad físicas, lógicas y administrativas, en concordancia con los riesgos inherentes al acceso a dicha información. Estas medidas estarán detalladas en un procedimiento interno que será de estricto cumplimiento para garantizar una adecuada protección de los datos personales.

Manejo de Imágenes y Material Audiovisual

La E.S.E. Santiago de Tunja informa sobre la implementación de mecanismos de seguridad a través de sistemas de video vigilancia, garantizando la protección de los derechos y la seguridad de pacientes, acompañantes, empleados y visitantes. Estos sistemas están instalados en diversas áreas de las instalaciones y oficinas de la entidad. La información recopilada a través de estos sistemas se utiliza exclusivamente con fines de seguridad de las personas y de los bienes e instalaciones. En caso de ser necesario, esta información puede ser presentada como evidencia ante autoridades competentes. Además, se realiza un respaldo periódico de los registros para asegurar su disponibilidad en caso de requerirse como prueba en procesos judiciales.

Suministro de información personal a autoridades judiciales o administrativas.

Cuando las autoridades o administrativas en ejercicio de sus funciones legales o judiciales soliciten a la E.S.E. Santiago de Tunja, el acceso y/o entrega de datos de carácter personal contenidos en cualquiera de sus bases de datos, se realizará la entrega de la información siguiendo estrictos procedimientos y garantizando la protección de los derechos de privacidad de los titulares de datos.

La justificación de esta medida se fundamenta en la necesidad de colaborar con las autoridades y administrativas en el cumplimiento de sus funciones legales o judiciales. La entrega de los datos personales solicitados se llevará a cabo previa verificación de la legalidad de la petición y la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad competente.

Es importante destacar que este proceso de verificación tiene como objetivo salvaguardar los derechos fundamentales de los titulares de datos, evitando cualquier uso indebido o abusivo de la información personal. Al realizar una evaluación minuciosa de la legalidad y pertinencia de la solicitud, la E.S.E. Santiago de Tunja garantiza el cumplimiento de las normas de protección de datos y preserva la confidencialidad y seguridad de la información personal de los individuos involucrados.

Asimismo, al asegurar que la entrega de datos personales se realice de manera responsable y acorde con los principios de proporcionalidad y finalidad, se contribuye a fortalecer la confianza de los titulares de datos en la gestión de su información por parte

de la E.S.E. Santiago de Tunja, fomentando así la transparencia y el cumplimiento normativo en materia de protección de datos.

Protección de la propiedad intelectual

- Los contenidos del sitio web son propiedad de la E.S.E. Santiago de Tunja o están debidamente autorizados por los autores intelectuales de dichos contenidos. En caso de utilizar información de fuentes externas, se hará referencia a la fuente correspondiente.

- Los contenidos del sitio web que sean de autoría ajena a la E.S.E. Santiago de Tunja estarán protegidos por las leyes colombianas en materia de derechos de autor, así como por las normas internacionales de Copyright. Se respetarán los derechos de autor y se tomarán las medidas necesarias para garantizar la legalidad en el uso de dichos contenidos.

- El incumplimiento de las políticas de privacidad, las condiciones de uso y los derechos de propiedad intelectual puede conllevar medidas que van desde la restricción del acceso al sitio web hasta acciones disciplinarias o legales, de acuerdo con lo establecido por la legislación aplicable en cada caso. Se velará por el cumplimiento riguroso de estas políticas con el fin de salvaguardar los derechos de todos los implicados.

5. RESPONSABILIDAD

Es responsabilidad de la alta gerencia y de todos los colaboradores de la E.S.E. Santiago de Tunja garantizar la implementación de las políticas de tratamiento de datos para mejorar las garantías de derechos de los titulares de datos personales y promover la transparencia en el manejo de la información.

6. DISTRIBUCION

Realizar amplia difusión de dichos objetivos a todos los colaboradores de la entidad, a los contratistas y personal tercerizado para su conocimiento y el logro de dichos objetivos.

CONTROL DE CAMBIOS

FECHA	VERSIÓN.	DESCRIPCIÓN DEL CAMBIO
08/08/2019	0	Elaboración y actualización del formato
01/04/2021	1	Actualización sistema de información dinámica gerencial
20/12/2022	2	Actualización licenciamiento sistema de información
02/02/2023	3	Actualización de la Política De Tratamiento De Datos Personales de la E.S.E Santiago de Tunja