



## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PG002-P07-PE

Versión: 01

2021-01-29

## TABLA DE CONTENIDO

|  |    |
|--|----|
| 1. PRESENTACION.....   | 4  |
| 2. ALCANCE.....  | 4  |
| 3. OBJETIVOS .....   | 4  |
| <b>3.1. Objetivo general</b> .....   | 4  |
| <b>3.2. Objetivos específicos</b> .....  | 4  |
| 4. MARCO NORMATIVO .....   | 4  |
| 5. TERMINOS Y DEFINICIONES.....  | 5  |
| 6. POLITICAS DE SEGURIDAD DE LA INFORMACION. ....  | 6  |
| 6. RESPONSABLES.....   | 7  |
| 7. METODOLOGÍA DE IMPLEMENTACIÓN.....  | 8  |
| <b>7.1. ACTIVIDADES Y ENTREGABLES DE LAS FASES DE LA METODOLOGÍA DE IMPLEMENTACIÓN.</b><br>.....     | 8  |
| 8. PLANES, PROCEDIMIENTOS Y CONTROLES. ....  | 10 |
| <b>8.1 CONTROL DE ACCESO</b> .....   | 10 |
| <b>8.2 PLAN DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO</b> .....                       | 10 |
| <b>8.3 MANEJO DE CONTRASEÑAS PARA ADMINISTRADORES DE TECNOLOGÍA</b> .....                            | 11 |
| <b>8.4 POLÍTICA DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL – LAN)</b> .....                 | 12 |
| <b>8.4.1 SEGREGACIÓN EN REDES</b> .....  | 13 |
| <b>8.4.2 CONTROL DE ACCESO REMOTO</b> .....  | 13 |
| <b>8.5 POLÍTICAS ESPECÍFICAS PARA USUARIOS DE LA DIRECCION TERRITORIAL DE SALUD DE CALDAS.</b> ..... | 13 |
| 9. CIFRADO .....   | 13 |
| <b>9.1 . POLÍTICA DE CONTROLES CRIPTOGRÁFICOS</b> .....  | 13 |
| 10. SEGURIDAD FÍSICA Y AMBIENTAL .....   | 14 |
| <b>10.1 POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO</b> .....                   | 15 |
| <b>10.2 POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS</b> .....  | 15 |
| <b>10.2.1 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA</b> .....   | 16 |
| <b>10.3 POLÍTICA DE MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS</b> .....                    | 17 |
| 11. SEGURIDAD DE LAS OPERACIONES DE TIC .....  | 17 |
| <b>11.1 GESTIÓN DE CAMBIOS:</b> .....  | 18 |

|  |    |
|--|----|
| <b>11.2 PROCEDIMIENTO DE GESTION DE CAPACIDAD:</b>   | 18 |
| <b>11.3 PROCEDIMIENTO DE SEPARACIÓN DE AMBIENTES:</b>  | 18 |
| <b>11.4 PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS:</b>                                     | 19 |
| <b>11.5 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN:</b>  | 19 |
| <b>11.5.1 RESPONSABILIDAD DE LAS COPIAS DE SEGURIDAD DE LA INFORMACIÓN:</b>                            | 19 |
| <b>11.5.2. Procedimientos de respaldo.</b>   | 19 |
| <b>11.5.3 Prioridad de la información para las copias de seguridad.</b>                                | 20 |
| <b>11.5.4 Política para realización de copias en estaciones de trabajo de usuario final</b>            | 21 |
| <b>11.6 Política de registro y seguimiento de eventos de sistemas de información y comunicaciones.</b> | 22 |
| <b>11.7 Política de control de software operacional.</b>   | 22 |
| <b>11.8 Política de gestión de vulnerabilidades</b>  | 23 |
| <b>12. SEGURIDAD DE LAS TELECOMUNICACIONES</b>   | 23 |
| <b>12.1 POLÍTICA PARA LA TRANSFERENCIA DE INFORMACIÓN.</b>   | 23 |
| <b>12.2 POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO</b>  | 24 |
| <b>12.3 POLÍTICA DE USO DE MENSAJERÍA INSTANTÁNEA Y REDES SOCIALES.</b>                                | 24 |
| <b>13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.</b>                         | 25 |
| <b>14 RELACIONES CON PROVEEDORES Y TERCEROS</b>  | 26 |
| <b>14.1 POLÍTICA DE TERCERIZACIÓN U OUTSOURCING</b>  | 26 |
| <b>15. MARCO LEGAL</b>   | 27 |

## 1. PRESENTACION

Este documento se realiza con el fin de dar a conocer cómo se llevara a cabo la implementación y socialización del sistema de gestión de seguridad y privacidad de la información dentro de la Dirección Territorial de Salud de Caldas.

## 2. ALCANCE

El plan de Seguridad y privacidad de la información se aplicará a los 12 procesos que hacen parte del mapa de procesos definidos en el sistema de gestión de calidad de la Dirección Territorial de Salud de Caldas.

## 3. OBJETIVOS

### 3.1. Objetivo general

Describir las actividades del plan de seguridad y privacidad de la información, para así establecer las medidas de índole técnica y organizacional, para así proteger, preservar y administra la confidencialidad, integridad, disponibilidad, y autenticidad requeridas para garantizar una adecuada seguridad y protección de la información de todos los procesos y procedimientos de la Dirección Territorial de Salud de Caldas.

### 3.2. Objetivos específicos

- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.
- Identificar los conocimientos y tecnologías que se requieren para la implementación de este proyecto, Investigar aplicaciones y servicios en telecomunicaciones para llevar a cabo la migración de servicios que se requieren para la privacidad de la información.
- Dar cumplimiento a lo establecido en el manual de gobierno digital emitido por el ministerio de tecnologías de la información y las telecomunicaciones.

## 4. MARCO NORMATIVO

La elaboración de este plan se soporta en las diferentes leyes, decretos y resoluciones que sugiere el MINTIC en su política de Gobierno Digital y que se listan en la siguiente tabla:

| NORMA  | DESCRIPCIÓN   |
|--|---|
| Ley 1273 de 2009                                 | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.   |
| Decreto Nacional 1377 de 2013                    | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.   |
| Ley 1581 de 2012                                 | Por el 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. Dar cumplimiento al modelo integrado de planeación y gestión en sus políticas gobierno digital, seguridad digital, transparencia, acceso a la información pública   |
| Decreto Nacional 103 del 20 de enero de 2015     | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.   |
| Ley 1753 de 2015                                 | Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país"  |
| Decreto 415 de 2016- DAFP                        | Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.   |
| Resolución 2710 de 2017 - Mintic                 | Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.   |
| Decreto No.1008 del 14 de Junio de 2018 - Mintic | 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.   |
| CONPES   | Política Nacional de Seguridad Digital, se tiene como objetivo: "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país". |
| ISO27001   | Articular las acciones en temas de privacidad y seguridad de la información a la NTC ISO-IEC-27001:2013   |

## 5. TERMINOS Y DEFINICIONES

- **Activo:** Recurso del sistema de información o cualquier elemento que tenga valor para la organización.
- **Activo de Información:** Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la institución. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo de seguridad de la información:** Es el riesgo o la probabilidad que se presenta con una amenaza para causar una pérdida o daño en un activo de información; los daños son la pérdida, afectación, modificación de la información entre otros. También se debe tener en cuenta que el riesgo no solo son los aspectos mencionados anteriormente, sino cuando se aprovechan de la información que se tiene para beneficio de algo o alguien en específico.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3)
- **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas que toman las organizaciones y los sistemas tecnológicos, con el fin que la información pueda ser resguardar y protegida, buscando mantener la confidencialidad, la disponibilidad e integridad de los datos con los que cuenta.

## 6. POLITICAS DE SEGURIDAD DE LA INFORMACION.

*“Los lineamientos del Plan Nacional de Desarrollo motivan a las entidades públicas del orden nacional y territorial a utilizar el poder de las tecnologías de*

*información y comunicación -TIC, para mejorar la eficiencia y transparencia de la administración pública.”*

En dicho documento se define el programa de renovación de la administración pública y establece que la finalidad de la estrategia de Gobierno Electrónico es *“(... definir una política y un conjunto de instrumentos adecuados para el manejo de la información en el sector público, de modo que se garanticen plena transparencia de la gestión, alta eficiencia en los servicios prestados a los ciudadanos y en las relaciones con el sector productivo y condiciones adecuadas para promover el desarrollo interno y la inserción internacional. Esta política confiere sentido a la incorporación y al uso de la tecnología informática en el desarrollo de las operaciones de las entidades estatales, tanto en sus actividades internas como en sus relaciones con otras entidades públicas y privadas, con los ciudadanos y con el sector productivo”*.

Este documento busca establecer el ¿por qué?, ¿qué? y ¿cómo? resguardar la información que fluye a través de la plataforma tecnológica y sistemas de comunicaciones de la entidad, agrupando todas las normas y políticas relacionadas con éste, teniéndose en cuenta los niveles de seguridad recomendados por la norma ISO 27002”. **M01-P06-GAF Manual Políticas de Seguridad de la Información**

Basado en lo expuesto, la Dirección Territorial de Salud de Caldas (DTSC) se ha puesto en la tarea de implementar su Modelo de Seguridad y Privacidad de la información tomada como referencia de los lineamientos del Manual de Gobierno Digital definido por el Ministerio de la tecnología de la información y las comunicaciones

La Dirección Territorial de Salud de Caldas, se compromete a administrar los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables. De igual manera, promueve una cultura en seguridad para evitar y administrar incidentes que contribuyan a la mejora continua del Modelo de Privacidad y Seguridad de la información – MPSI

## **6. RESPONSABLES.**

- Comité de Gestión Institucional y desempeño.
- Oficina de Planeación y Calidad.
- Oficina de Control Interno
- Profesional Universitario responsable del proceso de administración y soporte de Hardware y Software.
- Ingenieros de Apoyo a la administración y soporte de Hardware y Software.

## 7. METODOLOGÍA DE IMPLEMENTACIÓN

La implementación del Sistema de gestión de seguridad y privacidad de la información, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), el modelo MSPI de MINTIC, el modelo integrado de planeación y gestión – MIPG y la norma ISO 27001:2013.



Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

### 7.1. ACTIVIDADES Y ENTREGABLES DE LAS FASES DE LA METODOLOGÍA DE IMPLEMENTACIÓN.

#### Fase I – Diagnostico



La Entidad cuenta con un centro de datos, este espacio físico aloja una infraestructura de virtualización y almacenamiento implementados con tecnología Hewlett Packard en el año 2014, con capacidad de crecimiento hasta 13 host físicos adicionales, con elementos de energía y ventilación redundantes, que permiten continuar trabajando ante la falla de alguno de estos componentes.

Esta infraestructura se encuentra en su etapa media de vida, ya que el fabricante Hewlett-Packard no tiene este tipo de servidores en fabricación y el soporte de piezas cada vez es más costoso y difícil de reemplazar piezas que por su uso presentan fallas. El cableado estructurado de categoría 6ª se encuentra en condiciones perfectas para garantizar que a los equipos de cómputo la red de datos llegue sin problemas.

## Fase II – Planeación

Dentro de esta fase se relacionan las siguientes actividades:

- Documentar la revisión de la política de protección de datos personales, la cual debe ir alineada con todos los procesos de la Dirección Territorial de salud de Caldas.
- Utilizar los resultados de la fase de Diagnóstico para elaborar la política de seguridad y privacidad de la información alineada con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, y a través de una metodología de gestión del riesgo.
- Realizar el inventario de activos de información.
- Ejecutar la política de tratamiento de datos personales.
- Elaborar el plan de comunicación, sensibilización y capacitación referente a las políticas, guías y manuales.
- Elaborar el Plan de Contingencia y Continuidad.
- Registro Nacional de Bases de Datos: Documento evidencia del registro de las bases de datos en la plataforma de la SIC.
- Ejecutar el plan de riesgos de privacidad de la información.

## Fase III – Ejecución

- Alinear la política de protección de datos a los contratos de prestación de servicios y de apoyo a la gestión, a la revisión de los riesgos y el tratamiento específico de los datos personales, verificación de ajuste con la seguridad y privacidad a lo largo de la Entidad y a su vez con el Registro Nacional de Bases de Datos.
- Se mantendrá actualizado el inventario de activos de información, así mismo se deberá tener una caracterización de sus propietarios, teniendo clara la clasificación enmarcada en los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. En tal sentido la Dirección Territorial de Salud de Caldas se encargará del etiquetado y manipulación de la información de acuerdo al esquema de clasificación definido en los estándares y en la normatividad vigente.
- La Dirección Territorial de Salud de Caldas elaborará un mecanismo que permita dar a conocer y empoderar a sus funcionarios y contratistas, las políticas, lineamientos, manuales y guías relacionadas a la seguridad y privacidad de la información. Estas acciones serán responsabilidad del área de Talento Humano y la Oficina Asesora de Prensa y Comunicaciones.
- Durante la vigencia 2021 se actualizará el plan de contingencia a los nuevos lineamientos brindados por MINTIC para incluir los riesgos que se presentan en la privacidad de la información.

## **8. PLANES, PROCEDIMIENTOS Y CONTROLES.**

### **8.1 CONTROL DE ACCESO**

La Entidad tiene definida las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de la DTSC, para directivos, funcionarios, contratistas y terceros.

La conexión remota a la red de área local de la DTSC debe realizarse a través de una conexión VPN (Virtual Private Network) segura, empleando los equipos de seguridad perimetral instalados en la Entidad y gestionados por el área de TIC. El acceso a terceros deberá ser aprobado por el Comité de Seguridad de TIC, y se llevará registro y auditoría por parte del Área de TIC.

El acceso a los activos de información de la Entidad por parte de terceros estará permitido únicamente previo análisis y autorización del Comité de Seguridad de TIC, el cual deberá establecer los requerimientos y procedimientos que debe cumplir la Entidad o usuario solicitante.

### **8.2 PLAN DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO**

Ningún usuario deberá acceder a la red o a los servicios TIC de la Entidad utilizando una cuenta de usuario o clave de otro usuario, pues esto lo haría corresponsable de la información a la que tenga acceso.

La Dirección Territorial de Salud de Caldas, suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, por el jefe inmediato o supervisor, entendiéndose que estas son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, empleando la mesa de ayuda del Sistema de Gestión de Calidad, en donde se llevará a cabo la validación de los datos personales.

Las claves o contraseñas deben tener las siguientes características:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas doce anteriores.

La contraseña debe cumplir con tres de los cuatro requisitos siguientes:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Números (0 a 9)
- Caracteres especiales no alfabéticos (Ejemplo: \*,!,\$,%,&)

Las cuentas de los usuarios que realicen más de tres (3) intentos fallidos de acceso quedarán deshabilitadas y los usuarios deberán solicitar su desbloqueo por la mesa de ayuda establecida en el Sistema de Gestión de Calidad.

El funcionario que disponga de usuario de acceso a los activos de información, será responsable de su uso, el cual es personal e intransferible.

## **8.3 MANEJO DE CONTRASEÑAS PARA ADMINISTRADORES DE TECNOLOGÍA**

Se debe garantizar que el ingreso a las consolas de gestión y administración de las diferentes plataformas de tecnología, se realice mediante el uso de las credenciales de los usuarios de directorio activo.

Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el área segura donde designe la Entidad, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando la situación lo amerite.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal del Área de TIC no debe dar a conocer su clave de usuario de los sistemas de información a terceros, sin previa autorización del Coordinador de TIC.

Los usuarios y claves de los administradores de sistemas y/o del personal del Área de TIC son de uso personal e intransferible.

El personal del Área de TIC debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la Entidad de acuerdo al rol asignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Coordinador de TIC o el Asesor para la de Seguridad de la Información en caso de ser diferente.

## **8.4 POLÍTICA DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL – LAN)**

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la entidad sin la previa autorización del Área de TIC.

Todos los puntos de red que se encuentren sin uso deberán ser desactivados de los interruptores de red, de forma que se impida la conexión de equipos no autorizados.

Todas las conexiones a redes externas a las que se accedan desde la red interna de la Entidad pasarán a través del equipo de Gestión Unificada de Amenazas - UTM (del inglés Unified Threat Management) que posee la Entidad. Ningún equipo deberá conectarse saltando este servicio de seguridad.

Los usuarios que tengan acceso a servidores con IP públicas por cualquier tipo de protocolo de conexión (FTP, SFTP, SSH) no pueden establecer conexiones a sitios de información privados, a menos que hayan sido aprobadas por el Área de TIC de la Entidad.

## 8.4.1 SEGREGACIÓN EN REDES

La infraestructura tecnológica de la DTSC que soporta las aplicaciones debe estar separada en segmentos de red físicos y lógicos que independicen los accesos de usuarios de acuerdo a los diferentes perfiles que se establezcan, esto es, independientes de los segmentos de red de administración, contratistas, invitados y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de los interruptores de núcleo y borde, equipos perimetrales e internos de enrutamiento y de seguridad.

## 8.4.2 CONTROL DE ACCESO REMOTO

La autorización para la administración remota de equipos o de la infraestructura de servidores por parte del equipo de ingenieros del área TIC o de terceros en caso de servicios tercerizados debe estar documentada y justificada por el Comité de Gestión y Desempeño Institucional, indicando la responsabilidad que tiene el funcionario a quien se otorga este permiso y las funciones que cumplirá.

## 8.5 POLÍTICAS ESPECÍFICAS PARA USUARIOS DE LA DIRECCION TERRITORIAL DE SALUD DE CALDAS.

Es responsabilidad del área TIC garantizar que los puertos físicos y lógicos de administración, gestión y configuración de las plataformas de infraestructura brinden acceso privilegiado y restringido solo al personal autorizado de forma que los sistemas de información estén siempre restringidos y monitoreados de accesos no autorizados que puedan vulnerar la seguridad.

## 9. CIFRADO

### 9.1. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

El acceso remoto a la red y a los servicios tecnológicos de la Entidad por parte de todos los usuarios se deberá realizar a través de canales seguros utilizando autenticación y

cifrado de los canales, de acuerdo a los lineamientos de acceso que implemente el área de TIC en sus equipos de seguridad perimetral.

Toda información sensible que se extraiga de los aplicativos misionales deberá estar cifrada para evitar que la misma pierda su confidencialidad.

## 10. SEGURIDAD FÍSICA Y AMBIENTAL

Todas las áreas destinadas al procesamiento, almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de comunicaciones y sistemas de información crítica, se consideran sitios de acceso restringido. Por tanto, se implementarán las medidas de control de acceso físico en el perímetro de tal forma que puedan ser auditadas, así como los procedimientos de seguridad operacionales que permitan proteger la información. Para ello se emplearán los formatos establecidos en el Sistema de Gestión de Calidad.

El Área de TIC debe tener implementados controles de acceso a los centros de datos y de comunicaciones de las diferentes sedes de forma que se impida el acceso de personas no autorizadas, que puedan vulnerar la seguridad de la Entidad. Se debe contar como mínimo con los siguientes elementos:

- Puerta cortafuego de acceso con chapa de seguridad.
- Sistema de control de acceso biométrico que garantice la entrada solo al personal autorizado por la coordinación del área de TIC.
- Elementos de seguridad que alerten en caso de aumento de temperatura o generación de fuego y humo (sistema de detección de incendio). Estos elementos deberán contar con el mantenimiento anual respectivo por parte de una empresa certificada en el fabricante del elemento de forma que se asegure su correcto funcionamiento.
- Elementos de extinción necesarios mínimos, según lo exija la normatividad del Sistema de Gestión de Seguridad y Salud en el Trabajo -SG-SST.
- Los centros de datos y de comunicaciones deben contar con elementos de control de temperatura y humedad (aires acondicionados e higrómetros) que mantengan la temperatura de operación de los equipos en las condiciones normales sugeridas por los fabricantes de los mismos. Estos equipos deberán contar con el mantenimiento anual respectivo que garanticen su correcto funcionamiento y extiendan su vida útil.
- Los Centros de Datos deberán contar con sistemas de respaldo de energía eléctrica redundante (UPS y Planta Eléctrica) con autonomía que garantice la continuidad del servicio en caso de cortes de energía o daños de la red eléctrica pública.

El cableado eléctrico de las oficinas y centros de datos y comunicaciones deberán cumplir con los estándares de cableado y de protección eléctrica vigentes en las normas colombianas y las internacionales para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores y equipos de cómputo. Los sistemas de

tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

Se realizará limpieza al menos una vez por mes en compañía de personal del área de TIC, que permita mantenerse libre de polvo y elementos contaminantes que puedan deteriorar la infraestructura de telecomunicaciones y servidores.

El Área de TIC debe mantener actualizado el programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las barreras de seguridad (perimetrales e internas) de las instalaciones pertenecientes a la Entidad.

Las Entidad deberá considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

## **10.1 POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO**

En las instalaciones del centro de datos o de los centros de comunicaciones, está terminante prohibido:

- Fumar o generar humo por algún medio.
- Introducir alimentos o bebidas
- Portar de armas de fuego, objetos corto punzantes o similares, que no son herramientas requeridas para trabajar.
- Mover, desconectar y/o conectar servidores, almacenamientos, equipo de cómputo o de comunicaciones sin autorización.
- Modificar la configuración de los equipos o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos sin autorización.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

## **10.2 POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS**

La Dirección Territorial de Salud de Caldas debe poseer la infraestructura necesaria, con el fin de actuar contra eventos que pongan en riesgo la integridad y confidencialidad de la información, y es así, que los equipos de cómputo están conectados a las



instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra, para evitar pérdidas o daños de la información como activo fundamental de la Entidad.

Está prohibida la conexión de elementos eléctricos a las tomas eléctricas regulados por parte de personal ajeno al área de TIC.

El resguardo de los equipos de cómputo deberá quedar bajo el área de TIC contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos, el inventario total y las características de cada uno.

Los ingenieros del área de TIC son los encargados de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo.

Se cuenta con una herramienta de seguridad integral con firewall y antivirus para cada equipo de la Entidad y para los servidores, con una consola centralizada de gestión que permite el monitoreo remoto de los equipos e informa acerca de las vulnerabilidades detectadas. Esto garantiza una protección adecuada, pero es deber del usuario estar atento a las recomendaciones que emita el área de TIC sobre ataques y otras amenazas, ya que no es posible garantizar una seguridad completa.

Los ingenieros de TI deben mantener informados a los usuarios y poner a disposición de los mismos, el software que refuerce la seguridad de los sistemas de cómputo pertenecientes a la Entidad. Los ingenieros del área de TIC no están autorizados a realizar mantenimiento o reparación a equipos de contratistas o terceros, estos se deben realizar por fuera de la entidad con el personal de confianza del contratista.

### **10.2.1 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA**

Los funcionarios, contratistas y terceros que tienen algún vínculo con Entidad, deben conservar su escritorio libre de información propia de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de la DTSC, deben bloquear la sesión de su computador en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de la DTSC deben cerrar las aplicaciones y servicios de red cuando ya no los requieran.

Al imprimir documentos con información pública reservada y/o pública clasificada (semi-privada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.



No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

### **10.3 POLÍTICA DE MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS**

La Entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por la Dirección Territorial de Salud de Caldas, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, sistemas de información, medios de almacenamiento, aplicaciones, cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de su misión institucional.

Se debe realizar la aplicación del procedimiento de respaldo de información y borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario o contratista haya sido retirado de la Entidad, de acuerdo a lo definido por la DTSC.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través del Área de Sistemas y será objeto de auditorías de seguridad mediante el módulo de prevención de pérdidas de datos de la Entidad.

## **11. SEGURIDAD DE LAS OPERACIONES DE TIC**

Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica.

Cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación. Para la gestión de las operaciones de la infraestructura de

procesamiento de información en la Dirección Territorial de Salud de Caldas, el líder del área de TIC, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.

## **11.1 GESTIÓN DE CAMBIOS:**

Todo cambio o modificación que afecte de forma significativa algún sistema de información en la Entidad deberá ser tratado y aprobado en el Comité de Seguridad TIC. Principalmente se debe asegurar la continuidad del negocio y evitar que se vea afectada la atención de usuarios. Se debe documentar el procedimiento planeado de forma que se justifiquen los cambios a realizar, el cual debe contener aspectos como identificación, registro de los cambios, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, socialización con las áreas afectadas por los cambios, procedimientos para revertir las modificaciones o cambios, entre otros aspectos.

## **11.2 PROCEDIMIENTO DE GESTION DE CAPACIDAD:**

Se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, eliminación de ambientes y sistemas en desuso, restricción de ancho de banda, entre otros procedimientos.

## **11.3 PROCEDIMIENTO DE SEPARACIÓN DE AMBIENTES:**

Todo desarrollo de sistemas de información que se realice dentro de la Entidad por parte de funcionarios, contratistas o terceros, deberán ser supervisados por parte del área de TIC y deberán autorizarse previamente en el comité de Seguridad de TIC. Los desarrollos de nuevos aplicativos deberán ejecutarse en ambientes controlados con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos. Se debe seguir un procedimiento de separación de ambientes (desarrollo y pruebas) que permitan realizar una transición hacia el ambiente de producción, teniendo en cuenta también la compatibilidad de estos desarrollos con los diferentes sistemas que cuenta la Entidad.

## **11.4 PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS:**

Este procedimiento indica como la Entidad realiza la protección de sus sistemas de información contra códigos maliciosos mediante el uso de los UTM y aplicativos de seguridad con que cuenta, como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo, entre otros.

## **11.5 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN.**

Esta política tiene como fin proporcionar los medios de respaldo y recuperación adecuados para asegurar que toda la información esencial y aplicativos, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la Entidad, sean respaldadas y puedan ser restauradas en caso de un incidente crítico.

### **11.5.1 RESPONSABILIDAD DE LAS COPIAS DE SEGURIDAD DE LA INFORMACIÓN.**

El coordinador del área de TIC determinará los requerimientos para resguardar cada aplicativo o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El coordinador de TIC dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la DTSC.

### **11.5.2. Procedimientos de respaldo.**

Los procedimientos que se establezcan para el resguardo de la información, deberán considerar los siguientes puntos:

- a) Definir un esquema de rótulo de las copias de resguardo para el caso de copia en cintas o DVD, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
- b) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
- c) Probar periódicamente los medios de resguardo.
- d) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.
- e) Semanalmente el personal responsable de la plataforma de respaldo y continuidad de la DTSC, verificarán la correcta ejecución de los procesos de copia, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.
- f) Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.
- g) El administrador de la plataforma de copia de seguridad de la Entidad, deben generar tareas de restauración aleatorias de la información que deben ser documentadas.
- h) La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de mesa de ayuda del sistema de gestión de calidad de acuerdo a lo establecido por la Entidad.

La información previamente definida y contenida en los servidores de DTSC, se respaldará de forma periódica, determinada según el procedimiento "Respaldo y Restauración de copias de seguridad" y los medios que se consideren necesarios se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo incendio, humedad, y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

### **11.5.3 Prioridad de la información para las copias de seguridad.**

Las copias de seguridad se priorizarán de acuerdo a la importancia que representa la información para la continuidad del servicio de la entidad:

Servidores:

- Bases de Datos.

- Almacenamiento de recursos compartidos.
- Aplicativos.
- Copia de seguridad S.O. de red y controladora de dominio.
- Equipos de cómputo y portátiles en el dominio:
- También se tendrán en cuenta las siguientes consideraciones:
- La información que se considera relevante para el funcionamiento de la entidad y que se encuentra en las diferentes carpetas de los equipos de cómputo, tendrá un límite de almacenamiento en los servidores para las copias de seguridad, por tanto, es responsabilidad de cada usuario (funcionarios y contratistas) depurar y escoger muy bien aquella información que se debe proteger. La calidad de la información respaldada será responsabilidad exclusiva de los usuarios.
- Las bases de datos de la Entidad serán respaldadas periódicamente en forma automática con la herramienta de continuidad y respaldo que posea la entidad, según los procedimientos sugeridos para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más servidores alojados en un lugar seguro que permitan tener contingencia y continuidad de negocio.
- De ser posible, los servidores de contingencia de Bases de Datos y aplicaciones estarán alojados con un proveedor externo con el cual se realice convenio.
- Los servidores de hosting de la página web se contratarán con un tercero para evitar saturación de tráfico de datos en la Entidad.
- Los demás respaldos (copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo, en bodegas con los estándares de calidad para almacenamiento de medios magnéticos.
- Para reforzar la seguridad de la información, los usuarios, deberán hacer respaldos de la información de sus discos duros de manera semanal, dependiendo de la importancia y frecuencia de cambio, en las unidades de almacenamiento asignadas por la Entidad en los servidores.
- El personal de tecnología de la entidad no podrá remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

#### **11.5.4 Política para realización de copias en estaciones de trabajo de usuario final**

- Todos los usuarios son responsables de realizar una copia de respaldo de su información de valor, confidencial o crítica a su cargo. Estas copias separadas deben ser efectuadas con frecuencia en la carpeta asignada en las unidades de almacenamiento compartido disponibles.
- El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos de seguridad para la Entidad al ser conectados a los computadores, ya que son

susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal.

- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por Entidad.
- Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.
- Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Entidad.

## **11.6 Política de registro y seguimiento de eventos de sistemas de información y comunicaciones.**

Los funcionarios y contratistas de la DTSC, deberán informar inmediatamente al Comité de Seguridad de TIC cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información a su cargo, o de la que tuviera conocimiento.

El Comité de Seguridad de la Información será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

## **11.7 Política de control de software operacional**

Los responsables de la administración de las plataformas de producción del área de TIC estarán obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.

No se permitirá la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción, a menos que sea autorizado por el Comité de Seguridad de TIC y el área de TIC.

No se permitirá el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado por el Comité de Seguridad de TIC y el área de TIC.

## 11.8 Política de gestión de vulnerabilidades

La DTSC, deberá implementar los lineamientos para gestión de vulnerabilidades. Una vez identificadas las vulnerabilidades técnicas potenciales, la DTSC, identificará los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

El Comité de Seguridad de TIC realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

## 12. SEGURIDAD DE LAS TELECOMUNICACIONES

La DTSC a través del Comité de Seguridad de TIC, identificará los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión sobre los servicios de red, incluyendo los mismos en los contratos establecidos con sus contratistas.

### 12.1 POLÍTICA PARA LA TRANSFERENCIA DE INFORMACIÓN.

- El Área de TIC, realiza el control del uso de sistemas de transferencia de archivos vía SFTP a terceros. Para el uso de este protocolo de transferencia se deberá contar con autorización del Comité de Seguridad de TIC.
- Adicionalmente se deberá indicar como se realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.
- Para el intercambio de información con terceros, se implementarán métodos de transmisión seguros a través de protocolos SFTP y conexiones mediante VPN, que puedan ser monitoreadas.
- La Entidad debe contar con un certificado de firma digital tipo token emitido por una entidad avalada por el organismo nacional de acreditación (ONAC), para firma del representante legal de la Entidad que garantice la autenticidad, veracidad y exactitud de la información que se firma digitalmente, ya que esta cuenta con el mismo valor probatorio y fuerza obligatoria de una firma manuscrita.
- La custodia del token estará bajo la responsabilidad del líder del área de TIC, quien se encargará de realizar la firma de los documentos que se requiera enviar a los entes de control.
- Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la



información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

## 12.2 POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO

Los ingenieros de TI se encargarán de asignar las cuentas a los usuarios para el uso de correo electrónico corporativo de la Entidad, de acuerdo con lo establecido en el Manual de Políticas de Correo Electrónico Corporativo.

La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

El nombre a emplear en las cuentas corresponderá con la función que desempeñe el usuario, con el fin de facilitar al público su comprensión y digitación. La longitud mínima de las contraseñas será igual o superior a ocho caracteres alfanuméricos, como se establece en el numeral 5.1.4.

Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la DTSC.

## 12.3 POLÍTICA DE USO DE MENSAJERÍA INSTANTÁNEA Y REDES SOCIALES.

La Entidad tiene implementado un sistema de mensajería instantánea a través de su intranet, dispuesta para uso de los funcionarios y contratistas, como medio de comunicación oficial dentro de la Entidad. Toda la información que se transmita por este medio es tomada como oficial y es propiedad de la Entidad.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la DTSC, que sea creado a título personal en redes sociales como: *twitter®*, *facebook®*, *youtube®*, *likedink®*, *blogs*, *instagram*, entre otras, se consideran fuera del alcance de las políticas establecidas y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.



Toda información distribuida en las redes sociales que sea originada por la Entidad, debe ser canalizada a través de la Oficina de Prensa y Comunicaciones, y deberá ser previamente autorizada por los subdirectores y líderes de área para ser socializadas y difundidas, empleando un vocabulario claro y de fácil comprensión por los usuarios.

### **13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.**

El desarrollo de tecnologías informáticas al interior de la Entidad o desarrolladas por terceros para la Entidad se deben orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones.

La supervisión y seguimiento a proyectos de infraestructura informática, deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado a la Entidad.

La supervisión de estos proyectos de desarrollo, deberán contar necesariamente, con un integrante del área de TIC y opcionalmente un profesional del área que está directamente relacionada con el uso final, que se encargue de validar los requerimientos funcionales.

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.

- Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento hasta el nivel de rutinas y procedimientos.
- Toda la información de la Entidad deberá tender invariablemente a ser operada a través de un mismo tipo de sistema manejador de base de datos, con el fin de beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla. Entre tanto las bases de datos de diferentes aplicativos deben funcionar a través de interfaces seguras entre ellas, en el caso que requieran compartir información.
- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de la Entidad. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Uno técnico que describa la estructura interna del sistema, así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema los procedimientos para su utilización.
- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (normas básicas de Auditoría y Control).
- Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

## **14 RELACIONES CON PROVEEDORES Y TERCEROS**

### **14.1 POLÍTICA DE TERCERIZACIÓN U OUTSOURCING**

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la Entidad.

Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la DTSC, las cuales deben ser divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la DTSC.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la DTSC. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de seguridad de TIC antes de iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de tercerización en el portal de contratación.

Los funcionarios de la DTSC que fungan como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

## 15. MARCO LEGAL

| Norma  | Descripción   |
|--|---|
| Ley 1273 de 2009                             | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. |
| Decreto Nacional 1377 de 2013                | Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.   |
| Ley 1581 de 2012                             | Por el 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 Nacional 103 del 20 de enero de 2015 | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.   |
| Ley 1753 de 2015                             | Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país"  |
| Decreto 415 de 2016-DAFP                     | Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.                 |
| Resolución 2710 de 2017 - Mintic             | Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.   |
| Decreto No.1008 del                          | 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   |

|                              |   |
|------------------------------|---|
| 14 de Junio de 2018 - Mintic | libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones.   |
| CONPES                       | Política Nacional de Seguridad Digital, se tiene como objetivo: “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”. |

- **Anexos:**
- Anexo 1: Cronograma Plan de Seguridad y Privacidad de la Información Vigencia 2021-Versión de aprobación: 01 del 29 de enero de 2021

ORIGINAL FIRMADO

**ISABEL CRISTINA MURILLO ARIAS**

Jefe Oficina de Planeación y Calidad

ORIGINAL FIRMADO

**LUISA FERNANDA MARIN URIBE**

Subdirectora de Gestión Administrativa

Elaborado por: Equipo de Tics