C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AÑO 2025

ALCALDÍA DE FUNZA

SECRETARÍA GENERAL

OFICINA DE RELACIONAMIENTO CON EL CIUDADANO

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

Contenido

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

1. Introducción

Dado que el Decreto 1078 de 2015 es un Decreto Ley que compila la normativa vigente para el sector de Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*, modificado por el Decreto 1008 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";* así pues, la Alcaldía de Funza por medio de la Secretaria General y la Oficina de Relacionamiento con el Ciudadano – Área TICS, tomando como el Modelo de Seguridad y Privacidad de la información – MSPI, de MINTIC ha determinado las actividades del Plan de Seguridad y Privacidad de la Información que contribuyan a mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital, así como la actualización y fortalecimiento de las políticas, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI, que permitan prestar servicios de confianza, generando protección de la información, gestionando los riesgos y los incidentes de seguridad digital.

2. Objetivo General

Establecer diagnóstico de mejora para determinar la implementación del Modelo de Seguridad y Privacidad de la Información, articulados con la NTC/IEC ISO 27001:2022

3. Objetivos Específicos

- Actualización y fortalecimiento de las políticas, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI.
- Gestionar la mitigación de los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

- Fortalecer las mejores prácticas de seguridad informática de los usuarios como protección de los datos de la Administración Municipal, aplicando los cuatro principios de la seguridad de la información : confidencialidad, integridad, disponibilidad y autenticidad.

4. Marco normativo

- NTC-ISO/IEC 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos
- NTC-ISO/IEC 27002 Tecnología de la información, Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información
- 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”.
- MSPI - Modelo de seguridad y privacidad de la información ministerio de tecnologías de la información y las comunicaciones - MINTIC
- Política de gobierno digital ministerio de tecnologías de la información y las comunicaciones - MINTIC
- Resolución número 00500 de marzo 10 de 2021 MINTIC Modelo de Seguridad y Privacidad de la Información
- Resolución No. 1030 de 2021 (15 de diciembre de 2021) Adopción del plan de seguridad y privacidad de la información

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

5. Glosario de términos

Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

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). Análisis de Riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

Bases de Datos Personales: conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los servicios de información que se encuentran interconectados.

Ciberespacio: físico y virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que se usa para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

Datos Personales Mixtos: para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Derecho a la Intimidad: derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo
cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

Ley de Habeas Data: se refiere a la Ley Estatutaria 1266 de 2008. Ley de Transparencia y Acceso a la Información Pública: se refiere a la Ley Estatutaria 1712 de 2014.

Medios de almacenamiento de información: son dispositivos que permiten guardar, leer y escribir datos. Los más comunes son los discos duros, los discos de estado sólido, las memorias USB, las tarjetas de memoria, discos ópticos. Además de los dispositivos de almacenamiento físicos, también existe el almacenamiento en la nube. Este tipo de almacenamiento permite acceder a los datos desde cualquier lugar con conexión a internet.

Mesa de transformación digital: Son representantes o funcionarios delegados que participan de reuniones previas a los comité Institucional de Gestión y Desempeño de la administración municipal para aportar ideas de mejora ante una problemática de un tema propuesto, han sido creadas a través del decreto 117 de 2023 por medio del cual se adopta el Decreto 1499 de 2017, "*se crean y reglamentan las mesas de trabajo adscritas al Comité Institucional de Gestión y Desempeño y se derogan algunas disposiciones".*

MIPG: Modelo Integrado de Planeación y Gestión, es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (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).

Responsable del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la Información: preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad Digital: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales. 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).

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. Alcance

La Alcaldía de Funza, a través del Área TICS - Oficina de Relacionamiento con el ciudadano de la Secretaría General, ha diseñado el Plan de Seguridad y Privacidad de la Información Digital aplicable a todos los funcionarios, contratistas, practicantes, proveedores, grupos de valor y la ciudadanía en general que en cumplimiento de sus funciones y necesidades compartan, utilicen, recolecten, procesen, intercambien o consulten la información, así como los entes de control, entidades relacionadas que accedan ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación o medio de almacenamiento de la información.

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

7. Roles y responsabilidades

Roles	Responsabilidades
Secretaria General – Oficina Relacionamiento con el Ciudadano – Área TICS	Actualizar anualmente el Plan de Seguridad y Privacidad de la Información.
	Socializar el Plan de Seguridad y Privacidad de la Información.
	Ejecutar las actividades del Plan de Seguridad de la Información de la Alcaldía de Funza.
Funcionarios y contratistas administración municipal	Participar de las actividades derivadas del Plan de Seguridad y Privacidad de la Información. Cumplir con las Políticas de Seguridad y Privacidad de la Información.
Grupos de Valor y Ciudadanía en general.	Cumplir con las políticas de seguridad y privacidad de la información.
Encargado del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales (de los ciudadanos, funcionarios, grupos de valor) Es responsable de • Garantizar la seguridad de los datos. • Actualizar, rectificar o suprimir los datos cuando sea necesario. • Atender las consultas y reclamos de los titulares de los datos. • Comunicar las violaciones de seguridad de los datos a los titulares.
Responsable del Tratamiento de Datos	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. Es responsable de • Decidir los fines del tratamiento de los datos • Determinar los medios para el tratamiento de los datos

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

	• Proteger y hacer seguimiento a las medidas de seguridad de los datos
Comité Institucional de Gestión y Desempeño	Aprobar Plan de Seguridad y Privacidad de la Información.
Oficina de Control Interno	Realizar la evaluación a los avances y cumplimiento al Plan de Seguridad y Privacidad de la Información.

8. Evaluación plan anterior

La oficina de Control Interno realizó el seguimiento a través de la Matriz consolidada de planes (Decreto 612-2018), para la vigencia 2024 con un resultado de avance del 97%, de acuerdo a lo evidenciado en el cuarto informe de Seguimiento al Cumplimiento del Decreto 612 de 2018, enlaces
https://www.funza-cundinamarca.gov.co/control/ii-informe-de-seguimiento-cumplimiento-al-decreto-612
https://docs.google.com/spreadsheets/d/157evamuQvA614BZut22CnoGLBTwS9kFb/edit?gid=1564826399#gid=1564826399

- Actualizar la matriz de requerimientos legales en el sistema de información KAWAK – Normograma.
- Se socializó el Plan de Seguridad y Privacidad de Información, en las inducciones y sensibilizaciones a los funcionarios de la Administración Municipal.

  https://drive.google.com/drive/folders/1yo_M95Qqij_cG3lknO3V5DtSqeH_6CZB?usp=drive_link

- Se realizó el autodiagnóstico de Seguridad y Privacidad de la Información.

Para la vigencia 2023 se obtuvo como resultado final un 100% de cumplimiento, se resalta que en la implementación del Plan de Seguridad y Privacidad de la Información se logró:

- Generar la política del sistema de seguridad y privacidad de la información
- Actualizar la matriz de requerimientos legales en el sistema de información KAWAK – Normograma.
- Se realizó el autodiagnóstico y pruebas de seguridad informática

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

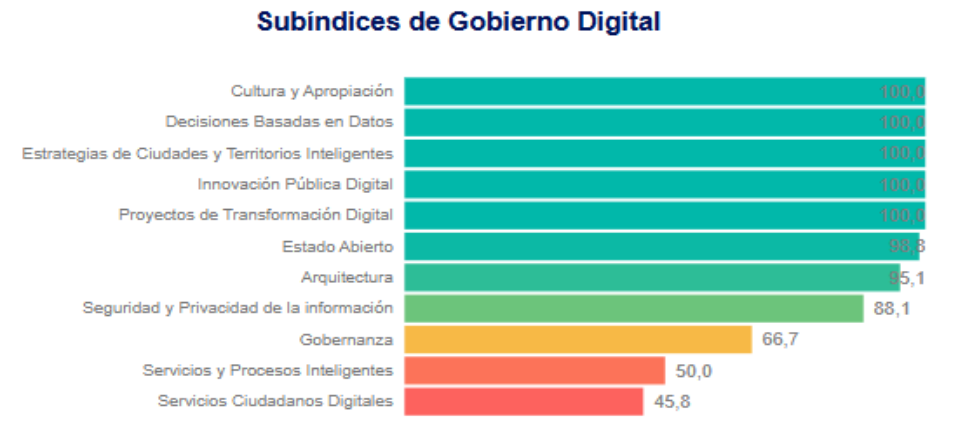
https://docs.google.com/spreadsheets/d/14CgQL2-nFDcNqJfq6Q-WlRxULIefKnc9/edit?usp=sharing&ouid=109005748311591606820&rtpof=true&sd=true

Resultado del ejercicio simulacro de Phishing

- **276** envíos al universo de colaboradores de ALFU **(100%)**.
- **248** mensajes enviados exitosamente **(89.9%)**.
- **154** personas leyeron/abrieron el correo **(62.1%)** *
- **122** usuarios no leyeron/abrieron el mensaje **(39.9%)** *
- **60** usuarios hicieron clic en el enlace **(24.2%)** *
- **28** mensajes rebotaron **(10.1%)**.
- **0** personas se des-suscribieron (retiraron) de la lista de envíos.
- **0** reportes de spam reportados.

- Se establecieron indicadores del sistema de seguridad y privacidad de la información

- Se logró subir el porcentaje de FURAG para la administración



C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

9. Contenido del plan

Con el ánimo de fortalecer la seguridad y privacidad de la información en la Administración Municipal, se determinaron las siguientes actividades de acuerdo a los recursos disponibles para la presente anualidad así:

ID	Actividad	Inicio	Fin	Responsables
1	Actualización Procedimiento Gestión de Incidentes de Seguridad de la Información	01/02/2025	30/03/2025	**Profesionales Área TICS**
2	Gestionar los incidentes de Seguridad de la Información Identificados	01/02/2025	31/12/2025	**Profesionales Área TICS**
3	Campañas publicitarias de los incidentes de Seguridad de la Información Identificados - Lecciones Aprendidas	01/02/2025	31/12/2025	**Profesional Asignado - Buen Gobierno - Comunicaciones Estratégicas**
4	Actualización Matriz de Requisitos Legales de Seguridad de la Información	01/02/2025	31/12/2025	**Profesionales Área TICS**
5	Actualización Plan de Continuidad del Negocio	01/02/2025	30/04/2025	**Profesionales Área TICS**
6	Actualización de las políticas de Seguridad y Privacidad de la Información	01/02/2025	30/04/2025	**Profesionales Área TICS**
7	Formular indicadores seguridad y privacidad de la información	01/02/2025	30/04/2025	**Profesionales Área TICS**
8	Implementación y monitoreo de indicadores seguridad y privacidad de la información	01/03/2025	31/12/2025	**Profesionales Área TICS**
9	Revisión de los controles ISO 27001:2022	01/03/2025	31/12/2025	**Profesionales Área TICS**
10	Ejercicio de identificación de vulnerabilidades y Hacking Ético	01/03/2025	31/12/2025	**Proveedor Externo**
11	Socialización políticas seguridad y privacidad de la información.	01/03/2025	31/12/2025	**Profesionales Área TICS**
12	Sensibilizaciones – capacitaciones de seguridad y privacidad de la información.	01/03/2025	31/12/2025	**Profesionales Área TICS**

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

10. Monitoreo, seguimiento y evaluación

El monitoreo y ejecución del presente Plan de Seguridad y Privacidad de la Información, es realizado en primera instancia por la Oficina de Relacionamiento con el Ciudadano de la Secretaría General, de acuerdo a las fechas establecidas y registrará los soportes correspondientes en el formato Matriz de Integración Planes Institucionales y Estratégicos 02 - FR – 110 ubicado en el siguiente enlace drive https://docs.google.com/spreadsheets/d/1xFL_FTMCFw5fJKFZegk1n9JBdVxJaY6n/edit?gid=1564826399#gid=1564826399

La Secretaría de Planeación y Ordenamiento Territorial realizará seguimiento de manera cuatrimestral, con fecha de corte a 30 de abril, 31 de agosto y el 20 de diciembre, durante los primeros 5 días después de la fecha de corte, o con una periodicidad menor de acuerdo con las instrucciones del Líder del Proceso o jefe de la dependencia.

La Oficina de Control Interno realizará evaluación de manera cuatrimestral, con fecha de corte a 30 de abril, 31 de agosto y el 30 de diciembre, una vez la Secretaría de Planeación y Ordenamiento realice el reporte.

11. Riesgos que pueden afectar el cumplimiento del Plan

En la siguiente tabla se relacionan aquellas situaciones que potencialmente puedan llegar a producir afectaciones negativas para el desarrollo del plan y sus objetivos.

Causa Raíz	Causa Inmediata	Descripción del Riesgo	Actividades de Control	Fecha	Responsable
Falta de recurso humano	Falta de seguimiento al plan.	Posibilidad de afectación económica o reputacional por falta de seguimiento del presente plan.	Contar con el personal para realizar el seguimiento.	03/01/25	Líder de Proceso

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

12. Aprobación, publicación y divulgación

El Plan de Seguridad y Privacidad de la Información es aprobado por el Comité Institucional de Gestión y Desempeño para ser publicado en la página web de la Alcaldía de Funza a más tardar el 31 de enero del año 2025.

Su divulgación se realizará aplicando lo establecido en la Política de Transparencia y Acceso a la Información Pública y el Plan de Comunicaciones de la Alcaldía de Funza, así como la Política de Responsabilidad con la comunidad y participación ciudadana.

13. Anexos:

- Matriz De Integración Planes Institucionales y Estratégicos 02 - FR – 110

14. Referencias bibliográficas y ciber biografías

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por 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 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 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.
- Decreto 029 del 4 de mayo de 2018, -"Por medio del cual se adopta el decreto 1499 de 2017 para la implementación del Modelo Integrado de planeación y Gestión (MIPG).
- Decreto 080 del 25 de septiembre del 2019 por medio del cual se crean las mesas de trabajo adscritas al comité institucional de gestión y desempeño (MIPG).

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

- Ley 1221 de 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- 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.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 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.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 de 2012. Por el cual se reglamenta parcialmente la Ley 1221 de 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- 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 1008 del 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.
- 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.
- Resolución 2133 de 2018. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se derogan las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27002:2015

C.P 250020
Tel. (601) 8234070
823 40 71 / 823 40 73
Fax. (601) 8257620
Dir. Cra. 14 No. 13-05

- Ley 1712 de 2014 Congreso de la República 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.
- Modelo de Seguridad y Privacidad de la información – MSPI MINTIC 2021 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf
- Resolución número 500 de Marzo 10 de 2021 MINTIC Modelo de Seguridad y Privacidad de la Información 2021 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
- Resolución 500 de 2021 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
- Modelo de Seguridad y Privacidad – MSPI – MINTIC https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_1.pdf
- Decreto 767 22 de mayo 2022 Política de Gobierno Digital MINTIC 2022
- Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas MINTIC 2018
- Decreto 080 de 2019 - por medio del cual se crean las mesas de trabajo adscritas al comité institucional de gestión y desempeño creado por el decreto 029 del 04 de mayo de 2018 y se modifican algunas de sus disposiciones.
- https://www.funza-cundinamarca.gov.co/normatividad/decreto-080-de-2019

Luz Angela González Mejia
Secretario de Despacho Secretaría General

	NOMBRE DEL FUNCIONARIO	CARGO	FIRMA	FECHA
Revisó:	Sandra Milena Rosas Rojas	Jefe Oficina Relacionamiento con el Ciudadano		Enero /25
Proyectó:	Juan Pablo Guzmán	Profesional Universitario		Enero /25
Proyectó:	Erika Buitrago Ramos	Profesional Universitario		Enero /25