

POLÍTICA DE SEGURIDAD DIGITAL

Dirección **Administrativa**



Vigencia

2026-2027



TRANS
MUSICAL
SETP



Alcaldía de
IBAGUÉ



1. Introducción

A partir del artículo 133 de la Ley 1753 de 2015 y del Decreto 1499 de 2017, el Modelo Integrado de Planeación y Gestión -MIPG- integró los sistemas de gestión de la calidad de la Ley 872 de 2003 y de Desarrollo Administrativo de que trataba la Ley 489 de 1998, siendo derogados los artículos del 15 al 23 de la Ley 489 de 1998 y la Ley 872 de 2003.

El MIPG 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 la ciudadanía, con integridad y calidad en el servicio. Entre los objetivos de la puesta en marcha de MIPG se destaca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza en sus entidades y en los servidores públicos.

En el artículo 2 de la Ley 2294 de 2023 — Bases del Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida" — se pretende sentar las bases para que el país se convierta en un líder de la protección de la vida, a partir de la construcción de un nuevo contrato social que propicie la superación de injusticias y exclusiones históricas, la no repetición del conflicto, el cambio en la forma de relacionarnos con el ambiente, y una transformación productiva sustentada en el conocimiento y en armonía con la naturaleza.

Para el SETP Transmusical de Ibagué, la información es el activo máspreciado de la entidad y, por tanto, se deben tomar todas las precauciones necesarias para mantenerla y preservarla. Para ello, el SETP ha venido desarrollando y evolucionando su modelo de seguridad de la información, soportado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad; adoptando buenas prácticas en cuanto a la gestión y administración de las tecnologías de la información.

De acuerdo con lo dispuesto en la política de Gobierno Digital, liderada por el Ministerio de las Tecnologías y las Comunicaciones -MinTIC- y reglamentada bajo el Decreto 767 de 2022, el SETP busca no solo que el uso de la tecnología sea ágil, sencillo y útil para los ciudadanos y usuarios del sistema de transporte, sino también que la interacción entre los diferentes actores involucrados se dé en un ambiente seguro, corresponsable y previsible. Esta política incluye como habilitador la seguridad de la información, junto con la arquitectura y los servicios ciudadanos digitales.

Con el fin de contribuir a la construcción de un Estado más participativo, más eficiente y más transparente, el SETP Transmusical de Ibagué, a través de la Oficina de TI y Sistemas de Información, ha venido recopilando las mejores prácticas nacionales e internacionales para definir los requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información -MSPI-, y para diseñar, adoptar y promover las políticas de seguridad digital en la entidad.

La planificación e implementación del MSPI en el SETP está determinada por la comprensión de la organización y su contexto, las necesidades y expectativas de los interesados, los requisitos de seguridad, los procesos misionales del sistema de transporte y el tamaño y estructura de la entidad. El MSPI conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos mediante la definición y aplicación de las políticas de seguridad, los roles y responsabilidades asociados, la identificación y clasificación de los activos de información y la definición de una metodología de gestión del riesgo.

La presente guía fue elaborada por la Dirección administrativa del SETP Transmusical de Ibagué. Contiene los siguientes elementos: objetivo de la guía, alcance, descripción de la política, marco de referencia, herramientas e instrumentos, definiciones, implementación de la política y aspectos con mayor potencial de desarrollo para las vigencias 2026-2027.

2. Objetivo de la Política

A través de la presente guía se definen las estrategias y mecanismos mediante los cuales el SETP Transmusical de Ibagué desarrolla e implementa la Política de Seguridad Digital, conforme a los lineamientos del MinTIC y el Modelo de Seguridad y Privacidad de la Información -MSPI-:

"El SETP Transmusical de Ibagué se compromete a implementar y propender por la preservación de los tres pilares fundamentales de la seguridad de la información — confidencialidad, integridad y disponibilidad —, gestionando y controlando la implementación de la seguridad digital al interior de la entidad por medio de la comprensión de las necesidades y expectativas de las partes interesadas, la determinación del alcance del Modelo de Seguridad y Privacidad de la Información -MSPI-, el liderazgo y compromiso de la alta dirección, la definición y seguimiento de las políticas de seguridad y privacidad de la información, la gestión de riesgos de seguridad digital y la definición de controles para su mitigación, todo ello alineado con la Política de Gobierno Digital y el MSPI del MinTIC."

Esta política es liderada a nivel nacional por el Ministerio de las Tecnologías de la Información y las Comunicaciones -MinTIC- y al interior del SETP Transmusical de Ibagué está a cargo de la Dirección Administrativa.

3. Alcance de la Política

La presente guía aplica a la a la Dirección Administrativa del SETP como líder de la política de Seguridad Digital, quien, en la implementación de dicha política y de acuerdo con el mapa de procesos vigente del SETP Transmusical de Ibagué, se encuentra inmersa en el proceso de Gestión de administrativa.

La política de Seguridad Digital aplica a todos los procesos, sistemas de información, infraestructura tecnológica y activos de información del SETP Transmusical de Ibagué, involucrando a todas las dependencias de la entidad como custodios y usuarios de la información institucional. En particular, involucra a:

- Gerencia General: Liderazgo y compromiso de la Alta Dirección del SETP con la implementación del MSPI. Aprobación de la política de seguridad digital institucional.
- Oficina de TI y Sistemas de Información: Dependencia líder de la política. Responsable del diseño, implementación, seguimiento y mejora continua del MSPI del SETP.
- Todas las dependencias del SETP: Custodios de los activos de información de la entidad. Responsables de aplicar los controles de seguridad definidos en sus procesos.
- Gestión Administrativa y Organizacional: Acompañamiento en la implementación del MSPI y articulación con las demás políticas del MIPG.
- Oficina Jurídica: Cumplimiento de los requisitos legales en materia de protección de datos personales (Ley 1581 de 2012) y delitos informáticos (Ley 1273 de 2009).
- Oficina de Control Interno: Seguimiento y evaluación al cumplimiento de los controles de seguridad digital y el MSPI del SETP.

4. Descripción de la Política de Seguridad Digital

Con la política de seguridad digital se pretende fortalecer las capacidades del SETP Transmusical de Ibagué para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades operativas, administrativas y en su entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al fortalecimiento de la confianza digital de los ciudadanos ibaguereños, los usuarios del sistema de transporte, los operadores y demás partes interesadas.

El SETP Transmusical de Ibagué se compromete a implementar y propender por la preservación de los tres pilares fundamentales de la seguridad de la información:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Garantizar que la información del SETP sea accesible únicamente a personas autorizadas, protegiendo	Garantizar que la información del SETP sea exacta, completa y no sea alterada de forma no autorizada	Garantizar que los sistemas de información y los datos del SETP estén accesibles y operativos

los datos de los usuarios, operadores y la gestión del sistema de transporte.

durante su creación, transmisión o almacenamiento.

cuando sean requeridos por los usuarios autorizados y la ciudadanía.

Para preservar estos tres pilares, el SETP se compromete a implementar los siguientes elementos del MSPI:

Compromiso MSPI	Descripción para el SETP
Comprensión de las partes interesadas	Identificar y analizar las necesidades y expectativas de las partes interesadas del SETP en materia de seguridad digital: ciudadanos, usuarios del sistema de transporte, operadores, entes de control, proveedores tecnológicos y servidores.
Determinación del alcance del MSPI	Definir el alcance del Modelo de Seguridad y Privacidad de la Información del SETP, identificando los procesos, sistemas de información, activos y la infraestructura tecnológica del sistema de transporte incluidos en el modelo.
Liderazgo de la Alta Dirección	La Gerencia General del SETP asume el compromiso explícito con la implementación del MSPI, otorgando los recursos necesarios y promoviendo la cultura de seguridad digital al interior de la entidad.
Políticas de seguridad y privacidad	Definir, socializar, aplicar y hacer seguimiento a las políticas de seguridad y privacidad de la información del SETP, incluyendo las políticas de uso de sistemas de información, contraseñas, clasificación de la información y protección de datos personales.
Roles y responsabilidades	Definir los roles y responsabilidades en seguridad digital de todos los servidores y contratistas del SETP, incluyendo la separación de deberes y el principio de mínimo privilegio en el acceso a sistemas de información.
Contacto con autoridades y grupos de interés	Establecer y mantener contacto con las autoridades pertinentes en caso de incidentes de seguridad digital: CSIRT Gobierno, COLCERT, Ministerio de Defensa y entidades de control, conforme al Decreto 338 de 2022.
Incorporación de la seguridad digital en proyectos	Garantizar que todos los proyectos de TI del SETP incorporen criterios de seguridad digital desde su diseño, incluyendo la evaluación de riesgos de seguridad en los proyectos de transformación digital del sistema de transporte.
Identificación y clasificación de activos	Inventariar, valorar y clasificar todos los activos de información del SETP (datos de operación, datos de usuarios, sistemas de gestión del sistema, plataformas de atención al usuario, infraestructura crítica) según su nivel de criticidad y confidencialidad.
Gestión de riesgos de seguridad	Identificar, valorar y definir el plan de tratamiento de los riesgos de seguridad digital del SETP, incluyendo los riesgos de ciberseguridad, fraude electrónico y compromiso de datos personales de los usuarios del sistema de transporte.
Definición de controles	Definir e implementar los controles técnicos, administrativos y físicos para la mitigación de los riesgos de seguridad digital del SETP, reduciéndolos a un nivel aceptable conforme al apetito de riesgo definido.

5. Marco de Referencia Normativo

A continuación, se enuncian las principales normas que regulan la Política de Seguridad Digital aplicable al SETP Transmusical de Ibagué:

Número	Año	Descripción
Ley 23	1982	Derechos de Autor. Protección de los activos de software del SETP Transmusical de Ibagué.
Constitución Política	1991	Artículo 15: Define el derecho a la intimidad y al buen nombre. Base constitucional de la protección de datos personales de los usuarios del SETP.
Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales.
Ley 594	2000	Ley General de Archivos. Marco de referencia para la gestión documental y la seguridad de los documentos del SETP.
Ley 603	2000	Protección de los derechos de autor en software. Obliga a las entidades a declarar si los programas de software que usan son legales.
Ley 962	2005	Simplificación y Racionalización de Trámites. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150	2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266	2008	Hábeas data y manejo de la información contenida en bases de datos personales.
Ley 1273	2009	Por medio de la cual se modifica el Código Penal creando el bien jurídico tutelado de la protección de la información y de los datos, y preservando integralmente los sistemas TIC.
Ley 1341	2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC.
Ley 1474	2011	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	2012	Por la cual se dictan disposiciones generales para la protección de datos personales de los usuarios y ciudadanos.
Decreto 2364	2012	Firma electrónica. Marco normativo para la validez de las actuaciones electrónicas del SETP.
Decreto 2609	2012	Gestión Documental. Por el cual se reglamenta el Título V de la Ley 594 de 2000 y parcialmente los artículos 58 y 59 de la Ley 1437 de 2011.
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 en materia de protección de datos personales.
Ley 1712	2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
Decreto 1078	2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854	2016	Política Nacional de Seguridad Digital. Marco de política pública para la seguridad digital en Colombia.
Resolución 500 — Anexo 1	2021	Por medio del cual el MinTIC actualiza el Modelo de Seguridad y Privacidad de la Información — Nuevo MSPI.
Decreto 338	2022	Por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de gobernanza de seguridad digital.

6. Herramientas e Instrumentos de Control

Para la correcta implementación de la política de seguridad digital por parte de la Dirección Administrativa del SETP Transmusical de Ibagué, se tendrán como punto de partida los documentos y herramientas que el MinTIC tiene a disposición, junto con el Anexo 1 de la Resolución 500 de 2021 — Nuevo Modelo de Seguridad y Privacidad de la Información -MSPI-. Todas las referencias a las políticas, definiciones o contenido relacionado están publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes.

Las principales herramientas e instrumentos para la implementación de la política son:

- Modelo de Seguridad y Privacidad de la Información -MSPI- del MinTIC: Marco de referencia para la implementación del sistema de gestión de seguridad de la información en el SETP. Disponible en: <https://www.mintic.gov.co/portal/inicio/Programas/Seguridad-y-Privacidad-de-la-Informacion/>
- Norma NTC ISO/IEC 27001:2013: Estándar internacional para el Sistema de Gestión de Seguridad de la Información -SGSI-. Marco técnico de referencia para el MSPI del SETP.
- Norma NTC ISO/IEC 27002:2013: Código de prácticas para los controles de seguridad de la información aplicables al SETP.
- Portal de Seguridad Digital del MinTIC: Guías metodológicas, lineamientos y herramientas para la implementación del MSPI. Disponible en: <https://gobiernodigital.mintic.gov.co>
- CSIRT Gobierno: Equipo de respuesta a incidentes cibernéticos del Gobierno colombiano, al cual el SETP debe notificar los incidentes de seguridad significativos. Disponible en: <https://www.csirt.gov.co>
- COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia, entidad de referencia para la gestión de incidentes de ciberseguridad de alto impacto.
- Formulario de autodiagnóstico MIPG del DAFP: Instrumento para evaluar el nivel de implementación de la política de seguridad digital en el SETP.
- Formulario FURAG: Herramienta del DAFP para la medición anual del Índice de Desempeño Institucional, con base en cuyos resultados se identifican aspectos de mejora de la política.
- Plan de Recuperación de Desastres -DRP-: Instrumento del SETP que define los procedimientos para garantizar la continuidad de los sistemas de información críticos del sistema de transporte ante eventos disruptivos.
- Guía de Administración del Riesgo de Seguridad Digital del DAFP: Marco metodológico para la identificación, valoración y tratamiento de los riesgos de seguridad digital del SETP.

7. Definiciones

Término	Definición
Activo de Información	En relación con la privacidad de la información del SETP, se refiere al activo que contiene información que la entidad genere, obtenga, adquiera, transforme o controle en su calidad de tal. Incluye bases de datos de usuarios, registros de operación del sistema, contratos y documentación institucional.
Amenaza	Causa potencial de un incidente no deseado que puede provocar daños a un sistema de información o a la organización. Ejemplo para el SETP: ataques cibernéticos a los sistemas de gestión del sistema de transporte. (ISO/IEC 27000)
Análisis de Riesgo	Proceso para comprender la naturaleza del riesgo de seguridad digital y determinar su nivel de criticidad en los procesos del SETP Transmusical de Ibagué. (ISO/IEC 27000)
Ciberseguridad	Conjunto de herramientas, políticas, conceptos de seguridad, controles, guías, métodos de gestión, acciones, formación y tecnologías aplicadas para proteger los activos de información del SETP en el entorno digital.
COLCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia. Entidad de referencia para la gestión de incidentes de ciberseguridad de alto impacto que afecten al SETP.
Confidencialidad	Pilar de la seguridad de la información que garantiza que los datos del SETP sean accesibles únicamente a personas autorizadas. (ISO/IEC 27000)
CSIRT Gobierno	Computer Security Incident Response Team del Gobierno colombiano. Equipo al cual el SETP debe notificar los incidentes de seguridad digital significativos.
Disponibilidad	Pilar de la seguridad de la información que garantiza que los sistemas y datos del SETP sean accesibles y operativos cuando sean requeridos por los usuarios autorizados y la ciudadanía. (ISO/IEC 27000)
DRP	Plan de Recuperación de Desastres. Instrumento del SETP que define los procedimientos para garantizar la continuidad de los sistemas de información críticos del sistema de transporte ante eventos disruptivos.
Estándar de Seguridad	Conjunto de características y requisitos de uso repetitivo y uniforme, de obligatorio cumplimiento para el SETP, que establece los controles mínimos de seguridad digital que deben implementarse en los sistemas de información de la entidad.
Incidente de Seguridad	Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del SETP y amenazar la seguridad de la información.
Integridad	Pilar de la seguridad de la información que garantiza que los datos del SETP sean exactos, completos y no sean alterados de forma no autorizada. (ISO/IEC 27000)

Lineamientos TIC	Directriz o disposición establecida por el MinTIC que debe ser implementada por el SETP para el desarrollo de la Política de Gobierno Digital, incluyendo la seguridad de la información.
MSPI	Modelo de Seguridad y Privacidad de la Información definido por el MinTIC. Se basa en los requisitos y controles definidos en la Norma NTC ISO 27001. Marco de referencia para la implementación de la política de seguridad digital en el SETP.
Plan de Tratamiento de Riesgos	Documento del SETP que establece las acciones, controles, responsables, plazos y recursos para tratar los riesgos de seguridad digital identificados, reduciéndolos a un nivel aceptable.
Seguridad de la Información	Habilitador de la Política de Gobierno Digital que busca que el SETP incorpore la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información e infraestructura, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información.
SGSI	Sistema de Gestión de Seguridad de la Información, enmarcado en la Norma Técnica Colombiana NTC ISO 27001. Marco de gestión del SETP para la administración sistemática de la seguridad de la información.
Vulnerabilidad	Debilidad en los sistemas de información, procesos o controles del SETP que podría ser explotada por una amenaza para comprometer la seguridad de la información de la entidad.

8. Aspectos con Mayor Potencial de Desarrollo — Vigencias 2026-2027

De acuerdo con los resultados de la gestión reportados a través del FURAG y el autodiagnóstico de la política de Seguridad Digital, el SETP Transmusical de Ibagué ha identificado los aspectos con mayor potencial de desarrollo para las vigencias 2026-2027. Los resultados de referencia por componente evaluado son:

8.1. Resultados por Componente de la Política

Indicador Global	Política de Seguridad Digital	Asignación de Recursos	Despliegue de Controles
Por determinar — IDI 2025	Por determinar — IDI 2025	Por determinar — IDI 2025	Por determinar — IDI 2025

8.2. Recomendaciones del DAFP para la Vigencia

El Departamento Administrativo de la Función Pública -DAFP-, con base en los resultados del FURAG, ha establecido las siguientes recomendaciones para la política de Seguridad Digital, aplicables al SETP Transmusical de Ibagué:

- Contar con un Plan de Recuperación de Desastres -DRP- definido e implementado para todos los procesos críticos del SETP, incluyendo los sistemas de gestión del sistema de transporte, las plataformas de atención al usuario y los sistemas de información operativos.
- Establecer, documentar e implementar un procedimiento para la gestión de seguridad digital (Ciberseguridad) del SETP que incluya la notificación a las instancias pertinentes (CSIRT Gobierno / COLCERT) ante incidentes de seguridad significativos, conforme al Decreto 338 de 2022.
- Proponer el diseño de un sistema para dar cumplimiento a la Ley de Protección de Datos Personales (Ley 1581 de 2012), en particular en lo relacionado con el tratamiento de los datos personales de los usuarios del sistema de transporte público de Ibagué.
- Fortalecer la implementación de los controles del MSPI en todos los sistemas de información del SETP, incluyendo los sistemas de gestión operativa del sistema de transporte.
- Desarrollar y ejecutar un programa de formación y sensibilización en seguridad digital dirigido a todos los servidores y contratistas del SETP, con énfasis en el manejo de datos personales de usuarios y en la prevención de incidentes de ciberseguridad.

8.3. Plan de Cierre de Brechas — Vigencias 2026-2027

Actividad	Producto	Líder Responsable	Fecha Propuesta de Ejecución
Contar con un Plan de Recuperación de Desastres -DRP- definido e implementado para todos los procesos críticos del SETP, garantizando la continuidad operativa del sistema de transporte ante eventos disruptivos.	Plan de Recuperación de Desastres -DRP- del SETP elaborado, aprobado por la Gerencia General e implementado. Pruebas del DRP realizadas al menos una vez por vigencia.	Dirección Administrativa	31 de diciembre de 2026 y 2027
Actualizar el procedimiento para la gestión de seguridad digital (Ciberseguridad) del SETP, garantizando que incluya la notificación al CSIRT Gobierno y COLCERT ante incidentes de seguridad significativos.	Procedimiento de gestión de ciberseguridad del SETP actualizado, publicado en el SIG y socializado con todos los servidores y contratistas.	Dirección Administrativa	31 de diciembre de 2026 y 2027
Proponer y desarrollar un plan de trabajo para el diseño de un sistema que garantice el cumplimiento de la Ley de Protección de Datos Personales (Ley 1581 de 2012) en el SETP, en particular en el tratamiento de datos personales de los usuarios del sistema de transporte.	Plan de trabajo para el diseño del sistema de protección de datos personales del SETP. Propuesta presentada al Comité Institucional de Gestión y Desempeño.	Dirección Administrativa / Oficina Jurídica	31 de diciembre de 2026 y 2027

Actualizar y fortalecer el inventario y clasificación de activos de información del SETP, incluyendo los sistemas de gestión operativa del sistema de transporte, las plataformas de atención al usuario y la infraestructura crítica de la entidad.	Inventario de activos de información del SETP actualizado y clasificado según criterios de confidencialidad, integridad y disponibilidad. Publicado en el portal institucional.	Dirección Administrativa	31 de diciembre de 2026 y 2027
Actualizar el plan de tratamiento de riesgos de seguridad digital del SETP, incluyendo los riesgos de ciberseguridad, fraude electrónico y compromiso de datos personales de los usuarios del sistema de transporte.	Plan de tratamiento de riesgos de seguridad digital actualizado. Controles definidos e implementados para los riesgos prioritarios. Informe de seguimiento semestral.	Dirección Administrativa	31 de diciembre de 2026 y 2027
Desarrollar y ejecutar un programa de formación y sensibilización en seguridad digital para todos los servidores y contratistas del SETP, incluyendo el manejo de datos personales de usuarios y la prevención de incidentes de ciberseguridad.	Al menos 2 jornadas de formación en seguridad digital por vigencia. Registros de asistencia. Evaluación de conocimientos. Campaña de sensibilización en seguridad digital.	Dirección Administrativa	31 de diciembre de 2026 y 2027
Implementar o actualizar las políticas específicas de seguridad y privacidad de la información del SETP, incluyendo la política de uso de sistemas de información, la política de contraseñas, la política de clasificación de la información y la política de protección de datos personales.	Políticas específicas de seguridad de la información del SETP publicadas en el SIG y en el portal institucional. Actas de socialización con todas las dependencias.	Dirección Administrativa	30 de junio de 2026 y 2027
Articular la Política de Seguridad Digital del SETP con la Política de Gobierno Digital, garantizando que todos los proyectos de transformación digital del sistema de transporte incorporen criterios de seguridad desde su diseño.	Protocolo de incorporación de seguridad digital en proyectos de TI del SETP. Al menos un proyecto de transformación digital con evaluación de riesgos de seguridad integrada.	Dirección Administrativa	31 de diciembre de 2026 y 2027

Control de Cambios

Versión	Fecha de entrada en vigencia	Naturaleza del cambio
1	Julio 2026	Se crea la Guía conforme a los lineamientos del MinTIC, la Resolución 500 de 2021 (MSPI), el CONPES 3854 de 2016, el Decreto 338 de 2022 y las particularidades institucionales del SETP Transmusical de Ibagué. Cubre las vigencias 2026-2027.