

VISIÓN GENERAL

Velar por la seguridad y privacidad de la información es una de las principales tareas de la Dirección de Tecnología e Innovación de la entidad, es por esto que se deben tener unas políticas claras y bien definidas con el fin de lograr este objetivo.

Con el fin de dar cumplimiento a todas las políticas, la Dirección de Tecnología e Innovación deberá definir las directrices técnicas, legales y administrativas que se requieran.

ALCANCE

El presente documento pretende definir las políticas, lineamientos, estrategias y prohibiciones que considera la entidad son necesarias para proteger la información de la entidad. Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del nombre de la entidad y la ciudadanía en general.

LINEAMIENTOS GENERALES DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Algunos de los lineamientos para tener en cuenta en la formulación de las políticas de TI son:

- **Responsabilidad**

El Director de Tecnología e Innovación en su calidad de tal, responde ante la Gerencia por la existencia y cumplimiento legal y de las medidas que mantengan un nivel de seguridad y privacidad de la información acorde con las necesidades de la entidad y los recursos disponibles.

- **Cumplimiento**

Estas políticas son aplicables a todos los empleados, contratistas, empleados en misión y practicantes, en adelante funcionarios, que de una u otra forma manipulen, procesen, almacenen cualquier tipo de información de propiedad de la entidad. La presente Política General de Seguridad y Privacidad de la Información entra en vigencia una vez aprobada por el Comité de Gestión y Desempeño de la entidad.

- **Excepciones**

Todas las excepciones a las políticas aquí descritas deberán estar definidas y aprobadas por la Dirección de Tecnología e Innovación de la entidad y deberán estar debidamente documentadas.

POLÍTICAS Y ESTÁNDARES

Las políticas y estándares de seguridad y privacidad de la información que se van a considerar son las siguientes:

- Políticas de clasificación de la información
- Políticas de manejo de la información impresa o en papel
- Políticas de manejo y uso de la información digital
- Políticas de control de acceso a la información
- Políticas de seguridad de los servicios de red
- Políticas de protección y respaldo de la información
- Políticas de seguridad física y entorno de la información
- Políticas de cumplimiento de normatividad
- Políticas de manejo de usuarios y claves de las redes sociales
- Políticas de seguridad de la información en la cadena de suministro de las TIC

POLÍTICAS DE CLASIFICACIÓN DE LA INFORMACIÓN

La entidad maneja múltiples tipos de información y lo primero que se debe tener en cuenta para protegerla es clasificarla de acuerdo con su tipo y uso, a continuación, se detallan estos:

- **Información Multimedia**

Por ser la entidad un canal de televisión, la información de audio y video es una de las más importantes y la que más demanda capacidad de almacenamiento. Esta información se caracteriza por un crecimiento diario y continuo y es usada por múltiples usuarios para diferentes fines.

- **Información de usuarios**

Es la información que generan todos los funcionarios en el desempeño diario de sus funciones principalmente se compone de documentos de texto, hojas de cálculo, presentaciones etc.

- **Bases de datos**

Esta es la información que generan los distintos aplicativos con los que cuenta la entidad, son de carácter contable, administrativo e informativo entre otros.

- **Información documental**

Esta es la información que se produce al digitalizar todos los documentos que entran y salen por el archivo documental de la entidad, básicamente se tratan de archivos de imágenes.

- **Aplicativos y contenidos web**

Esta información se compone de todos los instaladores de aplicativos propios, así como de todos los componentes de los distintos contenidos web de la entidad.

- **Correo electrónico**

Esta es la información generada por todos los correos electrónicos que envían y reciben los funcionarios de la entidad en sus cuentas institucionales.

POLÍTICAS DE MANEJO Y USO DE LA INFORMACIÓN IMPRESA O EN PAPEL

Todas las políticas relacionadas con el manejo y uso de la información impresa o en papel serán desarrolladas en el documento: “*POLÍTICA DE GESTIÓN DOCUMENTAL*”, el cual es desarrollado por el Archivo Documental de la entidad.

Además de lo anterior la Entidad formulo en el año 2025 la política de cero papel la cual establece los lineamientos y estrategias orientadas a la reducción del uso del papel en la Asociación Canal Local de Televisión – Telemedellín –, con el propósito de promover un uso racional de los recursos naturales, prevenir la contaminación ambiental, fortalecer la eficiencia de la gestión administrativa y avanzar en la migración hacia procesos digitales más ágiles y eficientes.

POLÍTICAS DE MANEJO Y USO DE LA INFORMACIÓN DIGITAL

Los funcionarios son responsables del correcto uso, manipulación y cuidado de la información con la que deban trabajar o tengan acceso.

Los estándares para el cumplimiento de esta política son:

- **Acceso a la información**

Todos los funcionarios tendrán acceso a los distintos tipos de información que requieran para desarrollar sus funciones, estos accesos serán otorgados

desde la Dirección de Tecnología e Innovación de acuerdo con las necesidades de cada uno de ellos y con las restricciones necesarias.

Las claves de acceso asignadas a los funcionarios son personales y no deberán ser compartidas con otros usuarios.

Los funcionarios deben procurar por cerrar las sesiones que tengan abiertas y desatendidas con el fin de proteger el acceso no autorizado a terceras personas.

Al finalizar la jornada laboral se deberán cerrar todas las sesiones y conexiones que se tengan abiertas.

Para solicitar el acceso a alguna plataforma de un funcionario se deberá usar el aplicativo *Solicitud recursos de TI*.

- **Manejo de la información**

Los funcionarios son responsables del correcto uso, manipulación y cuidado de la información con la que deban trabajar o tengan acceso. Cualquier uso indebido o no autorizado podrá ser sancionado de acuerdo al Manual de Políticas de TI o denunciado ante las autoridades competentes.

La manipulación de la información solo se podrá hacer por los canales autorizados por la entidad.

El uso de toda la información de la entidad es estrictamente para fines que tengan que ver con las tareas asignadas, en ningún caso podrá ser usada para beneficios personales, comerciales o de terceros.

La información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se deberá guardar bajo llave o en un gabinete u otro mueble de seguridad, especialmente cuando la oficina esté desocupada.

Al momento del retiro de un funcionario el área de Tecnología e Innovación deberá gestionar la información que deja la persona que se retira de la entidad para lo cual utilizará la información aportada en el formato de Paz y salvo que deben diligenciar los funcionarios.

En todo caso al asignar un equipo de cómputo a un nuevo funcionario, se debe garantizar la eliminación de la información de este.

- **Correo electrónico**

La entidad le facilita a cada uno de sus funcionarios una cuenta de correo electrónico la cual solo debe ser usada para fines institucionales.

A los empleados de planta y en misión no les está permitido el uso de sus cuentas personales para comunicaciones institucionales.

La protección de la información de los correos electrónicos institucionales es

únicamente de cada usuario el cual deberá tomar todas las medidas de seguridad para proteger dicha información.

Los funcionarios deben abstenerse de abrir archivos de dudosa procedencia que pongan en riesgo los sistemas de información de la entidad.

- **Sistemas de almacenamiento**

La entidad facilita a los usuarios sistemas de almacenamiento para guardar la información de acuerdo a su tipo, la mayoría de estos sistemas cuentan con copias de seguridad. Por lo anterior los funcionarios deben procurar almacenar toda la información que consideren importante en estos sistemas y evitar el almacenamiento local en las estaciones de trabajo, memorias USB y discos duros portátiles.

- **Uso del internet**

La entidad les facilita a todos sus funcionarios el acceso a internet, es obligación de cada uno hacer uso adecuado de este servicio evitando el acceso a lugares a sitios peligrosos y la descarga de archivos que no sean seguros y que puedan poner en riesgo la seguridad de la red y la información del Canal y por ende su información.

- **Disposición final de equipos**

La disposición final de equipos de cómputo, servidores, sistemas de almacenamiento se hará según lo indicado en la guía “*PROGRAMA DE MANEJO Y DISPOSICIÓN FINAL DE RESIDUOS DE APARATOS ELÉCTRICOS Y ELECTRÓNICOS*” (MA-GT-TE-08) en todo caso se deberá garantizar el borrado de toda la información almacenada en estos sistemas para lo cual se llevará un registro en la plataforma GLPI.

POLÍTICAS DE CONTROL DE ACCESO A LA INFORMACIÓN

La Dirección de Tecnología e Innovación debe implementar todos los controles necesarios para el acceso a la información en todos sus sistemas.

Los estándares para el cumplimiento de esta política son:

- **Usuarios y claves de acceso**

Para el acceso a muchos de los sistemas tecnológicos y de información de la entidad se implantará un acceso mediante usuario y clave, la cual deberá ser de uso personal y no podrá ser compartida salvo en los casos que lo determine la Dirección de Tecnología e Innovación.

Para algunos sistemas se crearán claves de acceso con distintos privilegios como usuario o administrador. De igual forma para cada usuario se definirán los niveles de permiso de acuerdo con la aplicación.

Las claves deben procurarse que sean lo más fuerte posibles combinando mayúsculas, minúsculas, números y signos.

La doble autenticación deberá ser aplicada en los siguientes casos: administradores de la plataforma de Google, administradores del Firewall, administradores de la consola de antivirus y por los usuarios de las VPN.

Toda la reglamentación para el manejo de usuarios y claves se regirá por el documento: POLITICAS Y PROCEDIMIENTOS DE GESTIÓN DE USUARIOS, CONTRASEÑAS Y PERFILES.

- **Directorio activo**

Con el fin de tener un control adecuado de usuarios y claves, la entidad cuenta con un sistema de directorio activo que permite centralizar las cuentas de los usuarios y aplicativos. En el momento del retiro del funcionario la cuenta será eliminada o suspendida en caso de que el retiro sea temporal.

- **Logs y registros de monitoreo**

La Dirección de Tecnología e Innovación tendrá un registro con el fin de monitorear las distintas actividades que se realicen con la información almacenada en los sistemas de la entidad.

Los sistemas que se consideran más críticos para llevar un control de los logs de registro son:

- Ofimática (aplicativo ERP)
- Control de acceso de funcionarios
- Firewall

Estos logs deberán ser almacenados por al menos 6 meses, entre los principales aspectos a controlar están: intentos de acceso no autorizado, cambios en la configuración del sistema, información transaccional entre otros.

POLÍTICAS DE SEGURIDAD DE LOS SERVICIOS DE RED

La Dirección de Tecnología e Innovación debe implementar todos los controles necesarios para garantizar la seguridad de los servicios de red.

Los estándares para el cumplimiento de esta política son:

- **Acceso a servicios de red**

Para el acceso a los servicios de SAMBA, SFTP, FTP, POP, IMAP, SMTP se deberá usar usuario y contraseña.

Las contraseñas para las conexiones por SAMBA importantes deben ser autogeneradas, con mayúsculas, minúsculas y de 8 caracteres

- **Firewall**

La entidad cuenta con un firewall de última generación con el fin de proteger el acceso externo a la información y bloquear los accesos no autorizados desde el exterior. La Dirección de Tecnología e Innovación definirá las reglas de acceso a los distintos puertos, así como como todas las restricciones que se considere tener con el fin de salvaguardar la información de la entidad.

En el Firewall la política debe ser denegar todo y permitir sólo lo estrictamente necesario, tanto para las conexiones entrantes como salientes

La entidad cuenta con un contrato de soporte con una empresa especializada que se encarga de la administración del Firewall.

- **VPN**

Se utilizarán para establecer conexiones remotas punto a punto cifradas. Mediante esta conexión los funcionarios podrán tener acceso a la red institucional de la entidad con el fin de que puedan desarrollar sus labores de forma remota. El servicio actual de VPN hace parte de los componentes del Firewall y es administrado por la misma empresa que gestiona este.

- **RADIUS**

Es el sistema de cifrado utilizado en las redes inalámbricas de la entidad.

- **Filtrado web**

La entidad realizara un filtrado web mediante el firewall con lo que se bloqueara el acceso a las siguientes categorías:

- Juegos
- Desnudez y riesgo
- Pornografía
- Citas
- Marihuana
- Abuso de drogas
- Hacking
- Ilegal o poco ético
- Discriminación
- Violenta explícita
- Grupos extremistas
- Proxy avoidance
- Plagio
- Lencería y bañador
- Abuso sexuales niños
- Otro material adulto
- Games
- Apuestas en línea
- Contenido pornográfico
- Juegos en línea

- **Servidor NTP**

El servicio de NTP debe estar implementado en todos los servidores de la entidad. El NTP del directorio activo será el que permite la sincronización de todos los equipos de cómputo.

POLÍTICAS DE PROTECCIÓN Y RESPALDO DE LA INFORMACIÓN

La Dirección de Tecnología e Innovación deberá tomar todas las medidas necesarias para proteger la información de cualquier tipo de amenaza o riesgo.

Los estándares para el cumplimiento de esta política son:

- **Antivirus**

Todos los equipos de la entidad que usen sistemas operativo Windows deberán estar protegidos con un software antivirus que los proteja de ransomware, malware y spyware, se exceptúan los que por sus condiciones operativas no lo puedan tener.

Los softwares antivirus de todos los equipos deben mantenerse actualizados y activos en todos los equipos.

La gestión del software antivirus se hará desde la consola que ofrece el fabricante para tal fin, desde esta se hará una revisión periódica de las actualizaciones, de las alertas y del correcto funcionamiento del sistema.

Periódicamente se programarán escaneos de los equipos con el fin de detectar posibles amenazas. Se realizarán auditorias con regularidad para evaluar periódicamente el desempeño del antivirus.

Todos los años se renovará la licencia del software antivirus.

- **Sistemas de almacenamiento**

Todos los sistemas que almacenen información como bases de datos, multimedia, archivos de usuario, imágenes deberán ser de tipo servidor y contar entre otras características con fuentes redundantes, niveles RAID 0, 1, 5, 6 y 7 (Raid Z 3), alta disponibilidad y capacidad de operación 24x7.

- **Enmascaramiento y criptografía de datos**

Con el fin de proteger los datos personales o confidenciales de la organización, la información de backups que se encuentre en discos duros extraíbles deberá estar cifrada, los backups de las bases de datos del ERP. El Director de Tecnología e Innovación es quien tendrá la custodia de las llaves para descifrar la información.

En cuanto a los backups en la nube se utilizará el cifrado por defecto que utiliza la plataforma de Google.

- **Backups**

Toda la información importante de la entidad estará protegida mediante backups de distintos tipos según el tipo de material. Los sistemas de backups son los siguientes:

- Disco óptico (ODA): Se utiliza como respaldo del material audiovisual almacenado en los servidores de archivo de la entidad (Delta). Este sistema fue remplazado por cintas LTO en el año 2024 pero continuara funcionando como un respaldo adicional de la información.
- Backups internos: Se usan para tener un backup de primera mano de los distintos archivos almacenados en los servidores. Estos backups se encuentran ubicados en el mismo servidor. Estos backups se sincronizan todas las noches.
- Equipos espejo: Se usan para respaldar la información de las bases de datos, aplicativos webs, imágenes archivo documental y la información de los usuarios que se encuentran almacenadas en los servidores de la entidad (Alpha y FOXTROT). Estos backups se sincronizan todas las noches.

- Discos duros portables: Se usan para respaldar la información del equipo espejo. Estos backups se sincronizan al final del mes.
- Backup en la nube: La entidad cuenta con un servicio de almacenamiento en la nube de Google con el fin de tener un backup de toda la información corporativa de la entidad.
- LTO: La entidad adopta a partir del año 2024 la tecnología de discos LTO para sus backups de archivos de video, los cuales se utilizarán como respaldo a los discos ópticos (ODA)
- En el siguiente link se puede observar como opera todo el proceso de backup de información de la Entidad.
<https://docs.google.com/drawings/d/1iLd6Z5d9omzrx3DBMudjLg3UiLutrCp5WWgE9OX6fo/edit>

Con el fin de comprobar la fiabilidad de los procesos de backups se deberá hacer una prueba mensual aleatoria de restauración de archivos, esta prueba deberá llevar un registro de quien la realizo y el resultado de la misma.

POLÍTICAS DE SEGURIDAD FÍSICA Y ENTORNO DE LA INFORMACIÓN

La Dirección de Tecnología e Innovación deberá tomar todas las medidas necesarias para proteger los entornos físicos donde se almacena la información.

Los estándares para el cumplimiento de esta política son:

- **Áreas seguras**

Se establecen como áreas seguras de la entidad las siguientes: Data center o CER, Master de emisión y Cuarto de control de cámaras. Estas son algunas normas que se deberán cumplir en estos espacios:

- El ingreso a estos espacios estará restringido mediante un sistema de control de acceso el cual sólo estará habilitado para el personal autorizado.
- Se deberá tener un control de las personas que ingresaron a estos espacios.
- No se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, amenos que se cuente con autorización para ello.
- El personal que ingrese deberá estar debidamente identificado.

- **Sistema eléctrico**

Todos los servidores de la entidad estarán protegidos mediante UPS's que garanticen el suministro permanente de energía y así evitar la pérdida de información por fallas del fluido eléctrico.

- **Redundancia de espacio**

Los sistemas para protección de información (backups) estarán ubicados en un lugar diferente de los servidores de almacenamiento, esto con el fin de evitar la pérdida de información por algún evento catastrófico en el data center o CER. Adicionalmente se cuenta con un servicio de backup en la nube.

- **Aire acondicionado**

Los sitios donde se tengan ubicados servidores que almacenen información deberán contar con un sistema de aire acondicionado que los proteja por posibles daños causados por un ambiente con temperatura muy alta.

- **Red contraincendios**

Los sitios donde se tengan ubicados servidores que almacenen información deberán contar con un sistema de red contraincendios que los proteja por posibles incendios.

- **Sincronización de relojes**

Todos los equipos de la entidad que se conecten a la red deberán tener sus relojes sincronizados mediante el protocolo NTP (Network Time Protocol)

POLÍTICAS DE CUMPLIMIENTO DE NORMATIVIDAD

La entidad dará cumplimiento a todas las normas que existan, estén vigentes y le apliquen sobre políticas de seguridad y privacidad de la información.

Los estándares para el cumplimiento de esta política son:

- **Protección de datos personales**

Para darle cumplimiento a la ley 1581 de 2012 de protección de datos personales la entidad expidió el “Manual de políticas de protección de datos personales”

- **Resolución 500 de marzo 10 de 2021**

Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

POLÍTICAS DE MANEJO DE USUARIOS Y CLAVES DE LA REDES SOCIALES

Cada día las redes sociales son más importantes en la operación de la entidad, así como en el cumplimiento de su objeto misional. Dado el alto impacto que tienen en la comunidad sus publicaciones, es de vital importancia proteger el acceso a todas estas plataformas con el fin de evitar accesos no autorizados o posibles hackeos de las cuentas.

Todas las políticas que se describen a continuación serán tenidas en cuenta en el documento **POLITICAS Y PROCEDIMIENTOS DE GESTIÓN DE USUARIOS, CONTRASEÑAS Y PERFILES.**

Los estándares para el cumplimiento de esta política son:

- **Usuarios**

Con el fin de tener un control de los accesos, ordenado, actualizado y riguroso de cada integrante, en un archivo digital compartido en Drive, donde estará la información de cada usuario, descrito de la siguiente forma: el nombre completo de cada usuario, el acceso a cada cuenta que requiere para su labor, tipo de equipo o dispositivo para uso de la cuenta, y novedades del uso de las misma.

Los usuarios del área Digital solo tendrán acceso a las cuentas en sus computadores de uso operativo del canal, se da excepción para instalarlas en los dispositivos móviles (celulares o tabletas) de uso personal, pero cada usuario velará por uso correcto y será responsable del manejo del mismo.

- **Claves**

Las contraseñas para el acceso respectivo a cada cuenta de las redes sociales se deberán cambiar de manera concurrente para lo cual queda estipulado cinco meses como mínimo, y la estructura para la creación de nuevas contraseñas será de la siguiente forma: tres bloques, con cuatro caracteres que contenga letras y números con símbolos, cada bloque separado por un espacio, también es motivo de cambio inmediato de las mismas, cuando se presente una alerta por intento de acceso externo no identificado.

Cada cuenta debe tener activa la seguridad de segundo paso o autenticación, o el tipo de seguridad máxima establecida por cada cuenta para evitar accesos externos no autorizados o algún tipo de fraude.

Todas las cuentas serán verificadas constantemente por los dos administradores y se realizara una abstracción de contenido a modo de respaldo, esto si en algún momento dado se presenta una eventualidad donde se requiera desbloquear alguna cuenta y a su vez se pueda demostrar con veracidad en datos la autoría de la misma.

Los códigos de acceso a cada cuenta envían para verificación llegara al número celular del área Digital, y de manera manual los administradores digitaran los accesos a los usuarios, no se podrá dejar ningún registro, ni guardar las contraseñas, ni nombre de usuario, en ningún equipo o dispositivo.

- **Gestión:**

La administración, los accesos, cambios, y niveles de seguridad de las contraseñas estarán a cargo de dos integrantes del área Digital, son los responsables de su manipulación y comportamiento de cada cuenta.

Los administradores de las contraseñas son los únicos autorizados para dar los accesos a cada integrante del área digital a cada una de las cuentas (redes sociales) que requiera para realizar su labor, los accesos se realizarían de manera manual en cada equipo por parte de dos administradores, esto con el propósito de llevar un control y seguimiento respectivo de los dispositivos con cuentas operativas.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LAS TIC

La gestión de la seguridad de la información en la cadena de suministro de las TIC es, cómo una organización maneja y protege la información que es compartida con terceros (proveedores, socios comerciales, subcontratistas, etc.) a lo largo de la cadena de suministro de tecnologías de la información y comunicación (TIC).

Es responsabilidad de la secretaria general incluir en todos los procesos contractuales las cláusulas que sean necesarias para hacer cumplir la política.

Los estándares para el cumplimiento de esta política son:

- **Contratos:**

Incluir en todos los contratos de la entidad cláusulas que obliguen a los contratistas a cumplir con el guardado del secreto y confidencialidad, así mismo se les debe socializar las políticas de seguridad de la información que tiene Telemedellín en la actualidad.

- **Riesgos:**

Identificación y evaluación de los riesgos asociados con los proveedores y los datos compartidos con ellos.

- **Evaluación de proveedores:**

La entidad debe procurar evaluar periódicamente a los proveedores de TIC para verificar su cumplimiento con los acuerdos de servicio y el cumplimiento del manejo de la información de la entidad.

REALIZÓ: CARLOS DUQUE CARGO: DIRECTOR TÉCNICO* FECHA: 10 de septiembre de 2019	REVISÓ: ANDRÉS JULIÁN PULGARÍN OROZCO CARGO: COORDINADOR SIGC FECHA: 16 de septiembre de 2019	APROBÓ: CARLOS DUQUE CARGO: DIRECTOR TÉCNICO* FECHA: 16 de septiembre de 2019
---	--	--

* El nombre del cargo fue cambiado en diciembre del año 2021 por Dirección de Tecnología e Innovación.

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	CAMBIOS REALIZADOS
V1	16/09/2019	Creación del documento
V1.1	24/02/2020	Revisión anual
V1.2	13/07/2020	Aprobación por el Comité de Desempeño
V1.3	22/02/2021	Revisión anual
V1.4	5/01/2022	Revisión anual
V1.5	13/01/2023	Revisión anual
V1.6	27/1/2023	Aprobación del comité de GYD
V1.7	26/7/2023	Inclusión de la política de seguridad de la información en la cadena de suministro de las TIC
V1.8	3/1/2024	Revisión anual
V1.9	20/5/2024	Ajuste lineamientos MINTIC
V2.0	20/08/2024	Ajustes auditoria RF y NISIT 2024
V2.1	3/01/2025	Revisión anual
V2.2	5/01/2026	Revisión anual