VISIÓN GENERAL

Cada día las herramientas de TI juegan un papel más importante en el quehacer diario de las empresas. Es por esto que su uso debe estar reglamentado mediante unas políticas claras acordes a la naturaleza de la entidad y sus necesidades. Estas políticas deberán ser continuamente revisadas para adaptarse a los cambios tecnológicos y a los requerimientos que se vayan presentando en la organización. Siempre se deberá buscar la optimización del uso de los recursos de TI siguiendo los principios de innovación, calidad, eficiencia, seguridad y confiabilidad.

ALCANCE

El presente manual pretende definir las políticas, lineamientos, estrategias y prohibiciones y sanciones que considera la entidad son adecuados para el correcto uso de sus recursos, aplicativos y demás herramientas de TI con las que cuenta.

LINEAMIENTOS GENERALES DE LAS POLIÍTICAS DE TI

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

- Responsabilidad
  Es responsabilidad de la Dirección Técnica definir todas las políticas y estándares que se deben cumplir para el correcto uso de las herramientas de TI. De igual forma debe velar por el cumplimiento de las mismas.

- Cumplimiento
  Estas políticas son aplicables a todos los empleados, contratistas, empleados en misión y practicantes, en adelante funcionarios, que usen las herramientas de tecnologías de información y la comunicación de la entidad. En caso del no cumplimiento de estas, la entidad tomará las medidas disciplinarias, contractuales y sancionatorias que se requieran.

- Excepciones
  Todas las excepciones a las políticas de TI deberán estar definidas y aprobadas por la Dirección Técnica de la entidad.

POLÍTICAS Y ESTÁNDARES DE TI

Las políticas de TI que serán adoptadas por la Telemedellín son:

- Política de adquisición, implementación y mantenimiento de las TI
- Política de uso de los servicios tecnológicos.
- Política de gestión de servicios de información
- Política de manejo y protección de la información
- Política de gestión del riesgo TI
- Política de trabajo en casa
- Política de seguridad de la información
- Políticas de sanciones

Política de adquisición, implementación y mantenimiento de las TI

La Dirección Técnica es el área encargada de gestionar la adquisición, implementación y mantenimiento de todos servicios tecnológicos y de información de la entidad, buscando siempre cumplir los principios de innovación, calidad, eficiencia, seguridad, confiabilidad y transparencia.

Los estándares para el cumplimiento de esta política son:

- **Requerimientos tecnológicos**
  Las Direcciones o áreas que tengan algún requerimiento tecnológico lo deberán solicitar al director del área a la que pertenezcan, y este lo deberá solicitar a la Dirección Técnica mediante correo electrónico o comunicación escrita.

- **Desarrollo de aplicaciones**
  La Dirección de Planeación apoyará en el diseño, contratación e implementación de aplicaciones que requiera la entidad.
  La propiedad intelectual de los desarrollos contratados será propiedad de la entidad, a menos que se defina lo contrario de forma escrita.

- **Compra de tecnología**
  Todas las compras de tecnología deberán ser hechas por la Dirección Técnica y priorizadas de acuerdo con la disponibilidad de recursos.
  La Dirección Técnica definirá el mecanismo de contratación de acuerdo con el manual de contratación de la entidad.

La compra de tecnología deberá estar alineada con los proyectos y fechas definidos en el PETI.

- **Mantenimiento de equipos**
  La Dirección Técnica es la encargada de planear y ejecutar los mantenimientos preventivos y correctivos de todos los equipos del Canal, con excepción de los sistemas propios del edificio donde actuará como asesor técnico.
  Los funcionarios tienen prohibido realizar cualquier tipo de mantenimiento a los equipos del Canal, en caso de incumplimiento serán sancionado de acuerdo con las políticas de sanciones definidas en este documento.

- **Garantía de equipos**
  Todos los equipos deben ser adquiridos con una garantía mínima de un año contra defectos de fabricación.
  Los equipos de cómputo se deberán comprar con una garantía de 3 años directamente con el fabricante y esta deberá estar registrada en la página web de este.
  Para casos puntuales como servidores, switches de red, etc, la entidad considerará la adquisición de planes de garantía extendida, debido a la criticidad de la operación de estos equipos.

Política de uso de los servicios tecnológicos

Todos los funcionarios que hagan uso de los servicios tecnológicos serán los responsables del adecuado uso y manejo de estos, y están obligados a cumplir todas las políticas y estándares fijados por la entidad.

Los estándares para el cumplimiento de esta política son:

- **Uso de los equipos**
  Los equipos propiedad de la entidad deberán ser usados solamente en actividades propias de ésta y en ningún caso para actividades personales de los funcionarios.
  Los funcionarios son los responsables por el correcto uso y cuidado de los equipos que tengan a su cargo y deberán responder por los daños o perdidas que les causen a estos de forma injustificada, en los casos que aplique

podrán ser sancionados de acuerdo con las políticas de sanciones definidas en este documento.

- **Instalación de software**
  La Dirección Técnica es la encargada de llevar el control de todas las licencias de software con las que cuente la entidad, este se realizará con un aplicativo que permita conocer toda la información de la misma, como donde está instalada, fecha de vencimiento, versión, etc.
  Los funcionarios no están autorizados para instalar ningún tipo de software en los equipos de la entidad, quien incumpla con esto podrá ser sancionado de acuerdo con las políticas de sanciones definidas en este documento.
  Todos los equipos deberán tener una clave de administrador con el fin de evitar que los usuarios puedan instalar cualquier tipo de software.
  En caso de que Telemedellín sea sancionado porque le encuentran un software ilegal, se podrá trasladar la sanción al causante.

- **Cuidado de los equipos**
  No está permitido pegarle ningún tipo de adhesivo a los equipos de la entidad.
  No está permitido el consumo de alimentos y bebidas en las salas de edición, master de emisión, CER y controles de estudio.
  Se debe procurar no consumir líquidos cerca de los equipos de cómputo.
  Se debe evitar poner en situaciones de peligro los equipos de la entidad.
  El funcionario que no cumpla estas normas podrá ser sancionado de acuerdo con las políticas de sanciones.

- **Reporte de daños y perdida de equipos**
  Los funcionarios que detecten una falla en un equipo deberán reportarla en el formato diseñado para tal fin (FT-GT-TE-01).
  Los funcionarios que dañen o extravíen un equipo deberán reportarlo en el formato diseñado para tal fin explicando detalladamente lo sucedido. (FT-GT-TE-01)
  Quien no informe oportunamente de la falla de un equipo será responsable de las situaciones que esto pueda generar.
  El funcionario que no cumpla estas normas podrá ser sancionado de acuerdo con las políticas de sanciones.

- **Reporte vulnerabilidades de seguridad**

  Todos los funcionarios que usan los servicios tecnológicos y sistemas de información de la entidad, deberán informar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

- **Custodia de los equipos**

  A los funcionarios que les sea asignado un equipo de forma transitoria o permanente serán los responsables de la custodia de este.
  Los usuarios de equipos portátiles deberán hacer uso de una guaya de seguridad.
  No está permitido el retiro de equipos de las instalaciones de la entidad sin el respectivo permiso, con excepción de los equipos que por su naturaleza son para uso externo.
  Antes de cualquier viaje al exterior el responsable del equipo deberá informar los equipos que salen del país para su respectivo reporte a la aseguradora.
  Siempre que se retire un equipo de almacén se deberá llenar el respectivo formato de préstamo de equipos donde quede claro a quién le queda cargado este.
  El funcionario que no cumpla estas normas podrá ser sancionado de acuerdo con las políticas de sanciones

- **Gestión de activos**

  Todos los equipos deben contar con una placa de inventario, ya sea de activo fijo, activo consumible o activo controlable.
  Cada equipo deberá contar con su respectivo registro u hoja de vida donde se lleve el historial de todas las actividades realizadas a este.
  La solicitud para ser dado de baja un equipo por fin de vida útil, desgaste u obsolescencia debe ser hecha por el Director Técnico.
  La Dirección Técnica definirá si un equipo luego de dar de baja se conserva ya sea para repuestos o para el Tour Telemedellín.
  Todos los equipos deben estar cubiertos con una póliza de seguros que los proteja frente a daño electrónico, robo o pérdida de acuerdo a la política de seguros del Canal.

Todos los equipos, repuestos, accesorios electrónicos y baterías que se desechen se les hará el correcto manejo para su reciclaje de acuerdo con el Programa De Manejo Y Disposición Final De Residuos De Aparatos Eléctricos Y Electrónicos de la entidad.

.

Política de gestión de servicios de información

Todos los funcionarios que hagan uso de los servicios de información serán los responsables del adecuado uso y manejo de estos, y están obligados a cumplir todas las políticas y estándares fijados por la entidad. La Dirección Técnica deberá garantizar el correcto funcionamiento de todos los servicios de información de la entidad.

Los estándares para el cumplimiento de esta política son:

- **Solicitud de recursos de TI**
  Cada Director o coordinador de área deberá hacer la solicitud de los recursos de TI mediante la herramienta dispuesta para esto en el portal de aplicativos de la entidad. Con esta herramienta se podrá solicitar: cuenta de correo electrónico, acceso a los aplicativos de la entidad, acceso a los sistemas de almacenamiento.

- **Correo electrónico**
  La entidad les asignara a todos los funcionarios una cuenta de correo electrónico que estará activa durante el tiempo que dure la vinculación de estos.
  El uso de esta cuenta es estrictamente institucional.
  La cuenta de correo electrónico será eliminada o desactivada una vez termine la vinculación con la entidad y de acuerdo con las fechas del formato de Paz y Salvo que deben tramitar todos los funcionarios.

- **Uso de aplicativos**
  La Dirección Técnica les dará acceso o instalará los aplicativos que requieran los funcionarios para el correcto desempeño de sus funciones.
  Los directores de área deberán solicitar a la Dirección Técnica la instalación de aplicativos especiales para sus funcionarios cuando ellos los requieran.
  El uso de los aplicativos es exclusivamente para temas laborales no está permitido el uso de estos para temas personales.
  La Dirección Técnica deberá llevar un control mediante una herramienta informática del uso y disponibilidad de aplicativos.
  El funcionario que instale software sin autorización de la dirección técnica, será sancionado de acuerdo a las políticas de sanciones de este documento.

- **Redes sociales**
  Las redes sociales solo podrán ser usadas para fines institucionales y de acuerdo con los lineamientos del coordinador digital.
  Es responsabilidad del coordinador digital el manejo de las claves de las distintas cuentas institucionales.

- **Versiones de software**
  La Dirección Técnica debe hacer todo lo posible en mantener actualizados los distintos softwares y aplicativos que se usen.
  Las actualizaciones de firmware o parches de software se deben hacer a versiones que garanticen la operabilidad del equipo y no ponga en riesgo la operación de la entidad.
  Se deberá validar con el fabricante del software la pertinencia de correr una actualización.
  Se deberá verificar la compatibilidad de las actualizaciones con otro software en uso.
  En los casos que se considere necesario y pertinente se deberán contratar planes de actualización de software de forma periódica.
  La Dirección Técnica deberá llevar un control mediante una herramienta informática de las versiones de software instaladas en cada equipo.

- **Uso de internet**
  No está permitido el acceso a páginas con contenidos no apropiados, y que no estén relacionadas con las funciones del trabajo. Por ética de trabajo y por seguridad de los equipos, está prohibido visitar páginas pornográficas y otras que por sus contenidos atentan contra la imagen y los principios del Canal.
  No está permitido descargar material de sitios poco confiables ya que la información descargada puede contener virus y poner en riesgo la estación de trabajo.
  Los funcionarios deben verificar antes de abrir archivos enviados por internet, ya que es muy común el envio de agentes maliciosos a través de este medio. En caso de considerarlos sospechosos deberá consultar a la Dirección Técnica para su verificación.

Política de manejo y protección de la información

La Dirección Técnica es la responsable de velar por el manejo y protección de la información digital de la entidad y para ello deberá tomar todas las medidas necesarias. Todos los funcionarios son responsables del correcto manejo de la información que usen para ejecutar sus distintas funciones.

Los estándares para el cumplimiento de esta política son:

- **Claves**
  A todos los funcionarios de la entidad se les asignará una clave para el acceso a todos los sistemas de información del Canal, esta clave es personal e intransferible y es responsabilidad de cada funcionario su correcto manejo. Las claves que se tienen establecidas son para los siguientes sistemas: correo electrónico, directorio activo, carpetas de usuario y aplicativos.

- **Almacenamiento local**
  Los funcionarios de la entidad podrán almacenar archivos localmente en sus equipos, pero esta información no estará protegida por backups y será responsabilidad de cada uno la perdida de información.

- **Carpetas de usuario**
  La Dirección Técnica les asignará a los funcionarios las carpetas que requieran en los distintos servidores de acuerdo a las necesidades de cada uno.
  Estas carpetas están protegidas por backups y solo podrán ser gestionadas o eliminar sus contenidos por el usuario.
  Solo está permitido el almacenamiento de información institucional.

- **Carpetas compartidas**
  La Dirección Técnica configurará las carpetas compartidas que sean necesarias para el correcto funcionamiento de cada área, es responsabilidad de cada director solicitar este servicio.
  Para la compartición de archivos existe una carpeta llamada TMP a la que tendrán acceso todos los funcionarios. El contenido de esta carpeta será eliminado los días lunes de todas las semanas.
  Está permitido el uso de carpetas compartidas mediante las herramientas que google tiene para esto siempre y cuando sean hechas con las cuentas oficiales de la entidad.

- **Discos duros portables y USB**
  La entidad les facilita a los funcionarios discos duros y memorias extraíbles tipo SD, USB, Compact Flash para almacenar la información que requieran, principalmente video. La información allí guardada será responsabilidad de cada uno de ellos por lo que deberán tomar las medidas de seguridad respectivas para salvaguardar dicha información. La entidad no tendrá restricciones en el uso de estos dispositivos, pero velará por su correcto uso.

- **Backups**
  La Dirección Técnica es la encargada de realizar todos los backups de información de acuerdo al manual de políticas de seguridad de la información.

- **Depuración de la información**
  Todos los funcionarios tienen la obligación de hacer una depuración permanente de la información almacenada en los distintos servidores.
  Al momento de terminar la vinculación con la entidad los funcionarios deberán entregar todas sus carpetas vacías y si es del caso transferirle los archivos al director del área a la que pertenezcan o a quien este designe.

Todos los detalles de los estándares de este lineamiento estarán contenidos en el documento Política de seguridad y privacidad de la información y en todos los documentos que hacen parte del MSPI (Modelo de Seguridad y Privacidad de la Información)

Política de gestión del riesgo TI

La Dirección Técnica es la encargada de realizar toda la gestión del riesgo de todos los servicios tecnológicos y de información de la entidad para lo cual debe identificar, calificar, priorizar y realizar el tratamiento de estos.

Los estándares para el cumplimiento de esta política son:

- **Mapa de riesgos**
  La Dirección Técnica es la encargada de crear y mantener actualizado el mapa de riesgos de TI de la entidad, así mismo de crear y ejecutar los planes de mitigación de riegos.

- **Manejo de riesgos y desastres**

Plan De Recuperación De Desastres Y Continuidad Del Negocio será la guía para el manejo y mitigación de riegos y desastres de la entidad.

Todos los detalles de los estándares de este lineamiento estarán contenidos en el documento Política de seguridad y privacidad de la información y en todos los documentos que hacen parte del MSPI (Modelo de Seguridad y Privacidad de la Información)

Política de seguridad y privacidad de la información

La Dirección Técnica es la encargada de garantizar las condiciones que se requieran para proteger y salvaguardar toda la información de la entidad.

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

Todos los estándares de este lineamiento estarán contenidos en el documento Política de seguridad y privacidad de la información y en todos los documentos que hacen parte del MSPI (Modelo de Seguridad y Privacidad de la Información)

Política de trabajo en casa

La entidad no tiene reglamentado el teletrabajo para sus funcionarios, pero si tiene la opción de trabajo en casa para los casos excepcionales que sean autorizados.

La Dirección Técnica es la encargada de fijar los medios tecnológicos mediante los cuales los funcionarios podrán desarrollar sus actividades laborales.

Los estándares para el cumplimiento de esta política son:

- Opciones de trabajo en casa
  Las modalidades que se tienen contempladas para el trabajo en casa son:

  1. Equipo de propiedad del Canal: En este caso se le llevara al domicilio del funcionario su equipo de trabajo y se conectara mediante una VPN a la red del Canal.
  2. Equipo propiedad del funcionario: En este caso se le dará acceso al funcionario mediante una VPN a la red del Canal o mediante un escritorio remoto dependiendo de las necesidades del usuario.

- Condiciones de uso con equipos de propiedad del Canal
  A continuación, se describen las normas que se deben cumplir cuando los funcionarios trabajan con equipos de propiedad del Canal.

  1. El equipo debe instalarse en un lugar seguro que evite daños por caídas, golpes o superficies inestables.
  2. El equipo es para uso exclusivo del funcionario de la entidad, en ningún caso debe ser manipulado o usado por familiares o amigos.
  3. El equipo es de uso exclusivo para la actividad laboral de cada funcionario y no debe ser usado para sus actividades personales.
  4. El funcionario deberá evitar consumir alimentos y bebidas cerca del equipo de cómputo.
  5. Cualquier fallo o problema técnico deberá ser reportado lo más pronto posible a la Dirección Técnica.
  6. Se le deberá reportar al seguro la dirección donde se tendrá instalado el equipo, así como el responsable del transporte de este.
  7. El funcionario deberá firmar un documento donde conste el recibo del equipo que se le está entregando.

- Condiciones de uso de la VPN
  A continuación, se describen las normas que se deben cumplir en el uso de las VPN.

  1. En la medida de lo posible se deberá usar conexión física para el internet con el fin de tener una mejor conexión y mayor seguridad.
  2. En caso de usar redes wifi estas deberán estar protegidas por clave de acceso.
  3. No se deberán usar redes abiertas de uso público.
  4. Se deberá cerrar la conexión luego de cada jornada laboral.
  5. Se deberá ser los más desconfiado y cauteloso en la apertura de correos electrónicos sospechosos, en caso de tener dudas podrán solicitar apoyó al personal del Área Técnica
  6. Se deberá evitar abrir páginas web no seguras y que no tengan que ver con las actividades propias del funcionario.

- Seguridad de la información

A continuación, se describen las condiciones para garantizar la seguridad de la información.

1. Procurar que toda la información sea almacenada en los servidores del Canal, ya sea en la carpeta de cada usuario o en la que por defecto tiene asignada el funcionario.
2. Cada funcionario es responsable del correcto uso de la información que esta manipulado o procesando.
3. Se deben cumplir todas las políticas de seguridad y privacidad de la información (MA-GT-TE-05).
4. Se debe evitar el uso de dispositivos de almacenamientos extraíbles tales como memorias USB o discos duros.

Políticas de sanciones

El Director Técnico, el jefe de Gestión Humana o el director del que dependa el funcionario o contratista que incumpla las políticas del presente podrán iniciar los procesos que consideren pertinentes con el fin de determinar las responsabilidades y posibles sanciones de acuerdo con los diferentes tipos de vinculación así:

- **Personal de planta**

  Tipo de proceso

  Llamado de atención verbal

  Proceso disciplinario

  Responsable

  Director del área o Control Interno Disciplinario

  Sanciones

  Las establecidas en el reglamento de trabajo y las demás contempladas por la ley.

- **Personal en misión**

  Tipo de proceso

  Llamado de atención verbal.

  Proceso disciplinario ante el empleador.

  Responsable

  Sera el Grupo técnico de apoyo al comité de gestión y desempeño integrado por: El Jefe de Gestión Humana (que lo convocará), El Secretario General y El Jefe de Control interno. Este el grupo técnico invitará al Director del área de la cual depende el funcionario y cuando lo considere necesario podrá invitar a las personas necesarias con el fin de determinar los hechos.

  Este grupo técnico de apoyo dará traslado a la empresa de servicio temporal que preste sus servicios a Telemedellín del informe realizado con el fin de que esta tome las medidas y sanciones requeridas.

  Sanciones

  Las sanciones las determinará la empresa prestadora de servicios temporales de acuerdo con la gravedad y la reiteración de las faltas. Podrán ser entre otras y dependiendo del reglamento interno de trabajo de esta, las siguientes:

  Llamada de atención por escrito con copia a la hoja de vida, por parte la empresa temporal

  Sanción disciplinaria de un día de suspensión (1) de trabajo.

  Sanción disciplinaria entre uno (1) y cinco (5) días de trabajo.

  Sanción económica.

  Terminación del contrato de trabajo por parte de la Empresa Temporal.

- **Contratistas**

  Tipo de proceso

  Llamado de atención verbal

Actuación sobre el contrato

Responsable

Supervisor del contrato y Secretaria General

Sanciones

Las contempladas en el contrato suscrito entre Telemedellín y el contratista.

Terminación anticipada del contrato.

Nota:

Para cualquier tipo de vinculación (de planta, en misión o por contrato) el canal podrá, adicionalmente, contemplar la posibilidad de instaurar acciones pecuniarias con el fin de resarcir los daños económicos generados a Telemedellín.

REALIZÓ: CARLOS DUQUE LÓPEZ **CARGO:** DIRECTOR TÉCNICO **FECHA:** 15 de agosto de 2019	**REVISÓ:** ANDRÉS JULIÁN PULGARÍN OROZCO **CARGO:** COORDINADOR SIGC **FECHA:** 20 de agosto de 2019	**APROBÓ:** DIEGO FLÓREZ LÓPEZ Y CARLOS DUQUE LÓPEZ **CARGO:** JEFE DE GESTIÓN HUMANA Y DIRECTOR TÉCNICO **FECHA:** 21 de agosto de 2019

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**CAMBIOS REALIZADOS**
V1	21/08/2019	Creación del documento
V2	3/04/2020	Actualización del documento
V3	26/10/2020	Actualización del documento
V4	8/10/2021	Actualización del documento