DESCRIPCIÓN GENERAL	
MACROPROCESO	Apoyo
NOMBRE DEL PROCESO	Seguridad y privacidad dela información
SUB PROCESOS	Realización y control de copias de seguridad
LIDERES DE SUB PROCESOS	Coordinador de Tecnologías
ÁREAS INVOLUCRADAS	Todas las Áreas de la Organización
OBJETIVO	Definir un conjunto de directrices, estrategias y pautas de acción para la protección y conservación de información, haciendo uso de una plataforma tecnológica estable y segura.
ALCANCE	Aplica para todos los procesos de la Organización, teniendo en cuenta el uso de los medios tecnológicos y sistemas de información para el cumplimiento de sus funciones.

I. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE SISTEMAS DE INFORMACIÓN

El presente documento contiene los lineamientos encaminados a resguardar adecuadamente los activos de información de Teleantioquia, en cada uno de los procesos definidos a continuación:

- *Respaldo de Información de sistemas de información*

Se elabora una copia de las bases de datos (sistemas de información), los archivos más relevantes de la Compañía y su configuración en unidades de cinta, con el fin de asegurar que la empresa pueda restaurar la información con un mínimo de pérdida, al presentarse una falla o catástrofe que imposibilite el funcionamiento de los Sistema.

Como parte de la caracterización de Gestión de Tecnologías de Sistemas de Información, se hace referencia a protección de la información de datos personales e información, así:

1. Se establece que todos los sistemas de información y bases de datos que procesen o almacenen datos personales, deberán contar con políticas de administración de claves de acceso y medidas de seguridad lógica.

2. Se cuenta con un Programa de Respaldo de Información de *sistemas de información,* en cintas LTO que contiene las Bases de Datos con la información de los sistemas de información del Canal.

3. Con la finalidad de contar con una plataforma de servidores estable y proceso de recuperación de desastres, se cuenta con servidor redundante en Servidores de administración de usuarios o Directorio activo para conservar los perfiles de Usuarios. adicionalmente, se cuenta con server de contingencia de Bases de Datos para posibilitar la continuidad y minimizar riesgos por perdida de funcionalidad o servicio.

4. Cada usuario es responsable de la información contenida en los bienes informáticos de cada Unidad, respaldando periódicamente la información pertinente a su cargo y en medio externo.

Integridad y oportunidad de la información

5. Cada usuario es responsable de los datos que, por sí, registre o procese en los diferentes sistemas y bases de datos del Canal, por lo que se considerará una responsabilidad administrativa:

   - La captura, envío o entrega de información incompleta, incorrecta o falsa.
   - La dilación intencional en la captura o registro de información en los sistemas y bases de datos.

Seguridad lógica de los sistemas y bases de datos

6. Los administradores de los sistemas y bases de datos deberán prever políticas de administración de claves de acceso y perfiles de usuarios.
7. Los usuarios, en todo momento, serán responsables del uso de sus claves.
8. Los respaldos previamente a su almacenamiento y resguardo, deberán ser analizados a fin de verificar que no contengan virus, gusanos o códigos maliciosos informáticos.
9. Los respaldos de información clasificada como reservada o confidencial, preferentemente, deberán tener una clave de acceso.

De la protección de los derechos de autor

10. Se promueve el estricto cumplimiento de la Ley en materia de derechos de autor en el Canal, por lo que:

    a. Queda prohibida la utilización de programas de cómputo (software) tanto operativos como aplicativos, ya sea en forma de código fuente o de código objeto sin su licencia de uso respectiva,

b. Así mismo, queda prohibida la descarga, almacenamiento, reproducción, transferencia y distribución de archivos, que contravenga y lesione los derechos de autor de cualquier obra protegida a través de tecnologías de información propiedad del Canal.
c. Corresponde a los responsables del proceso de tecnología, el control y resguardo de las licencias de programas de cómputo (software).

d. Los encargados de los procesos de tecnología son los responsables de realizar la instalación de programas de cómputo (software) en los equipos de cómputo. En caso de ser el Usuario quien instale programas de cómputo (software) en su equipo, éste será responsable del uso legal del mismo, así como de los daños y perjuicios que ocasione.

e. Queda prohibido el uso de dispositivos de almacenamiento y duplicadores de medios magnéticos (CD Writer, DVD Writer, cintas magnéticas, memoria flash, discos externos) para fines distintos al respaldo de datos e información.

11. Los usuarios del Canal, a los cuales se les ha asignado computador portátil y guaya deberán, en todo caso, utilizar la guaya de seguridad provista para la protección por pérdida o hurto del computador a su cargo.

12. Los usuarios del Canal, a quienes se les ha asignado computador portátil, serán responsables de mantener la confidencialidad y privacidad de la información Institucional contenida en el mismo, y serán los únicos responsables de mantener copias de seguridad en medios externos de la misma información.

Contratos de asesoría y servicios

13. Las propuestas de contratos de asesoría y servicios de informática deberán estar avalados, justificando la necesidad de los mismos

14. Los contratos para desarrollo de programas de cómputo o de asesoría y servicios de informática, deberán contar con la validación de la Dirección de Realización y Producción.

De los centros de cómputo

15. El Centro de Cómputo y CER son áreas restringida y por lo tanto sólo puede ingresar a ella personal con autorización del Director(a) de Realización y Producción, por el Coordinador de Tecnologías o por el funcionario encargado en caso de ausencia temporal o definitiva (mientras se provee el cargo) del jefe o por el funcionario encargado del proceso.

16. La operación de cualquiera de los dispositivos que en él se encuentran, solo podrá realizarse por los funcionarios de tecnologías o personal autorizado por los mismos.
17. Las personas que ingresen al Centro de Cómputo, deberán seguir las normas de seguridad que, para el efecto, se tienen previstas tales como:
    - No ingresar ningún tipo de bebidas o alimentos.
    - No accionar ninguno de los dispositivos de alarma sin razón evidente.
    - No encender cigarrillos, fósforos, encendedores o elementos que puedan ocasionar que las alarmas y sistemas de seguridad se accionen.
    - No conectar equipos de soldadura, aspiradora, brilladora.
    - No operar ninguno de los diferentes equipos que en él se encuentran instalados, sin autorización de Informática.

Del ingreso y retiro de personal

18. Ante el ingreso de personal al Canal que requiera para el cumplimiento de sus actividades de los servicios tecnológicos, Gestión Humana o quién haga sus veces, según sea la modalidad de contratación que se utilice, notificará si se dotará por parte de Teleantioquia de las herramientas para el cumplimiento del objeto contractual específicamente en Software y Hardware y, según las funciones desarrolladas, con qué sistemas de información tendrá interacción.

19. Parágrafo: la Coordinación de Gestión Humana o quién haga sus veces, en el término de tres (3) días hábiles anteriores, deberá informar a la Coordinación de Tecnologías o quién haga sus veces sobre el ingreso o retiro de personal que opera en el Canal y que requiera de servicios tecnológicos, sean por contratación directa o indirecta.

- **Respaldo de Información de Contenido audiovisual TN:**

20. Respaldo del Flujo Gestión de Contenido

Teleantioquia para la gestión y conservación de su contenido en formatos digitales cuenta con:
Un almacenamiento online de tráfico donde se sube el contenido en primera instancia.

Posterior y como primera medida de seguridad de la información, se realiza una copia en un almacenamiento intermedio Nearline.

para su conservación el contenido se almacena en el archivo profundo en medios de cintas LTO 7.

21. *Respaldo Flujo de Edición de Contenidos*

Teniendo la captura original del contenido que se requiere en edición, el productor o realizador se encarga de hacer una copia en un disco duro externo y posteriormente subir el material a un almacenamiento NAS dedicado para la edición del contenido

Una vez terminada la edición el contenido finalizado se envía al sistema de gestión de contenido para proceder con su conservación y futura emisión.

22. *Respaldo de contenidos en directo*

Los programas grabados en master o móvil, son capturados en formato digital. Posteriormente ingestados en el sistema de gestión de contenidos. Luego se realiza el proceso de conservación (*Respaldo del Flujo Gestión de Contenido)*.

23. Y demás acciones contenidas en el documento de Plan de Contingencias de Tecnología que propician condiciones favorables que minimizan los casos fortuitos que puedan poner en riesgo la información y estabilidad de la plataforma tecnológica.

II. POLÍTICA DE GESTIÓN DE USUARIOS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PERSONAL

1. OBJETIVO

Otorgar los lineamientos para la gestión de privilegios en los Sistemas de Información, el uso de equipos de cómputo, la retirada de los mismos y el almacenamiento de información en dispositivos extraíbles.

CONTENIDO DE LA POLÍTICA

Artículo primero: Responsabilidad de los usuarios. Todos los usuarios de los servicios de información –software- son responsables del manejo de sus datos de autenticación para el uso y acceso a los recursos informáticos de la SOCIEDAD TELEVISIÓN DE ANTIOQUIA LIMITADA. Los usuarios deben mantener en secreto su información de autenticación a los sistemas.

a. Los usuarios son responsables de todas las actividades realizadas con su identificador en la red ID.
b. Los usuarios deben hacer un correcto uso de la información a la cual tienen acceso.
c. Los usuarios no deben divulgar las claves de acceso o contraseñas de los dispositivos y sistemas informáticos de la organización.
d. Los usuarios pueden hacer uso de los datos e información contenidos en los recursos informáticos de la organización solo para fines laborales.

Artículo segundo: Gestión de privilegios. El responsable del Proceso de Tecnología de Sistemas de información, de la Información debe limitar y controlar el uso de privilegios a los usuarios mediante procesos de autorización formal, para evitar el uso inadecuado de privilegios y prevenir fallas en la operación de los sistemas de información.

a. Cualquier cambio en los roles y responsabilidades de los usuarios de la organización debe ser notificado al Proceso de Tecnología de Sistemas de información para realizar el respectivo cambio de privilegios.
b. El responsable del tratamiento de la información debe revisar que los privilegios asignados estén alineados con las necesidades del rol y las responsabilidades del usuario.

Parágrafo: Los privilegios se determinarán de acuerdo con los requerimientos administrativos de la organización, en tal sentido se establecerán de forma diferente para los Procesos Estratégicos, Misionales y de Apoyo.

Artículo tercero. Escritorios limpios.

a. Al momento de finalizar la jornada de trabajo, el funcionario debe guardar en un lugar seguro y bajo llave los medios que contengan información sensible de la organización.
b. En caso de ser necesario imprimir algún documento que contenga información clasificada o sensible, se debe retirar inmediatamente de la impresora y asegurarse que no haya quedado nada en cola de impresión.
c. No ingerir alimentos y bebidas en los puestos de trabajo.

Artículo cuarto. Pantallas limpias.

a. La pantalla de autenticación para el acceso a la red de la organización debe solicitar únicamente el ID de usuario y la contraseña.
b. Cuando el colaborador se ausente de su lugar de trabajo, debe bloquear su estación de trabajo de tal forma que proteja el acceso a las aplicaciones, servicios de la organización y archivos.

Artículo quinto. Retirada segura de equipos

a. En casos de almacenamiento de información que requiere niveles altos de seguridad (datos personales sensibles, información crítica de la organización) será necesario la destrucción total del soporte de almacenamiento.
b. Antes de que el equipo de cómputo sea cedido o desechado, además de realizar borrado seguro, también será necesario eliminar las carpetas temporales, los datos guardados en las cookies, los backups de los datos, configuración de cuentas de usuario y de correo. (Caso equipos de **cómputo leasing**).

Artículo sexto. Correo electrónico.

Cuando un colaborador o contratista de TELEANTIOQUIA realice el envío de correos electrónicos masivos (Boletín electrónico), deberá asegurarse que los destinatarios sean incluidos dentro de la etiqueta “Copia Oculta”. Lo anterior, evitando que datos personales semiprivados puedan ser conocidos por los destinatarios del correo. En tal sentido se debe hacer uso de la plataforma autorizada de envío de correo masivo con que cuenta el canal.

PLAN DE COMUNICACIONES

Las políticas de seguridad de la Información de Teleantioquia ha sido elaborado con la participación de los colaboradores de la unidad de Tecnologías y el apoyo de la Dirección de Producción y Tecnologías.

Este documento se ha socializado internamente con otras áreas del Canal, y se hace entrega de la versión revisada a Planeación para que sea publicado y esté disponible para todos, conforme con el decreto 612 para su divulgación.