TABLA DE CONTENIDO

## 1. OBJETIVO

Establecer las políticas en el uso correcto de los recursos y servicios de red e informáticos estableciendo las responsabilidades que debe seguir el usuario.

## 2. ALCANCE

Estas políticas están dirigidas a todos aquellos funcionarios de planta y contratista de Metroplús, que tienen responsabilidad con el uso y/o administración de los recursos informáticos institucionales (equipos, software, sistemas de información, Bases de Datos, conectividad, controles de acceso). Comprende el cumplimiento de los estándares de seguridad bajo las normas del Sistema de Gestión de Seguridad Informática SGSI ISO 27001, los requerimientos establecidos de seguridad por MINTIC y legislación vigente.

## 3. NORMATIVIDAD

**Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013:** Por la cual se dictan disposiciones generales para la protección de datos personales, Habeas data y seguridad de la información en datos personales.

**Decreto 2693 de 2012:** Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

**Decreto 2578 de 2012:** Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en

equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones.

**Decreto 2609 de 2012:** Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

**Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

**NTC ISO 27001:2013:** Sistema de Gestión de Seguridad de la Información (SGSI).

**Decreto 235 de 2010 (art. 1-4)**: Por el cual se regula el intercambio de información entre Entidades para el cumplimiento de funciones públicas.

**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.

**Decreto 2753 de 2014:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

**Decreto 415 de 2016:** Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.

**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.

**Ley 1928 de 2018:** "por medio de la cual se aprueba el «convenio sobre la ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest.

**ISO 27002:2013:** Norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.

**LEY 1336 DE 2009:** "por medio de la cual se adiciona y robustece la Ley 679 de 2001 de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

## 4. DEFINICIONES

**ACTIVO:** Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. Pueden ser tangibles o intangibles, incluye el software y hardware.

**AMENAZA:** Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos, que puede ser de origen interno o externo.

**ANÁLISIS DE RIESGO:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**ATAQUE:** Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema, que puede ser interno o externo y que busca afectar y desestabilizar los procesos de la entidad y poniendo en riesgo la información, los activos y el patrimonio de la entidad, de tal forma que su funcionamiento se ve afectado.

**DESASTRE INFORMÁTICO:** Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadores necesarios para la operación normal. La pérdida, robo o alteración de la información, se considera un desastre informático grave y se debe realizar una investigación exhaustiva que conduzca a tomar los correctivos del caso.

**HARDWARE:** Corresponde a todas las partes físicas y tangibles de un computador de oficina o portátil, que incluye sus partes eléctricas, electrónicas, electromecánicas y mecánicas con todos sus accesorios.

**RIESGO:** Es la probabilidad de que suceda un evento, impacto o consecuencia adversos para la plataforma tecnológica de Metroplús S.A y que puede poner en riesgo el normal desempeño de los procesos de la empresa.

**SEGURIDAD INFORMÁTICA:** Consiste en asegurar que los recursos del sistema de información (programas, aplicativos, bases de datos) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

**SOFTWARE:** Es el conjunto de programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación, llamado también soporte lógico del sistema.

**USUARIO:** Es la persona vinculada o contratista que tenga una cuenta de ingreso a la red de Metroplús S.A. y que para el desempeño de sus actividades necesite ingresar a los sistemas de información de la entidad.

**VULNERABILIDAD:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

**ÁREAS SEGURAS:** Lugares donde se encuentra localizada la información crítica para la organización, éstas estarán protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.

**BACKUP (COPIA DE RESPALDOS):** Copia de seguridad de los archivos, aplicaciones y/o bases de datos disponibles en un soporte magnético (generalmente discos o SAN), con el fin de poder recuperar la información en caso de un daño, borrado accidental o un accidente imprevisto.

**BASE DE DATOS:** Conjunto de archivos de datos recopilados, definidos, estructurados y organizados con el objeto de brindar información.

**CONFIDENCIALIDAD:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**CORTAFUEGOS (FIREWALL):** es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

**CONTRASEÑA:** Cadena de caracteres que permite validar la autenticidad de una cuenta de usuario.

**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.

**CONTROL CORRECTIVO:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

**CONTROL DETECTIVO:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

**CONTROL DISUASORIO:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

**CONTROL PREVENTIVO:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

**DISPONIBILIDAD:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

**EVALUACIÓN DEL RIESGO:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

**EVENTO DE SEGURIDAD DE LA INFORMACIÓN:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

**GESTIÓN DEL RIESGO:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

**LOGS:** Registro oficial de eventos, durante un rango de tiempo en particular, en donde se almacena toda actividad que se hace en el equipo monitoreado.

**NIVELES DE RESPALDO DE LA INFORMACIÓN:** Hace referencia a los diferentes ambientes en los cuales la copia de seguridad se guarda de manera oportuna con el fin de tener varios niveles de recuperación de la información en caso de desastre.

**NO REPUDIO:** El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

**PLAN DE CONTINGENCIA:** Procedimientos alternativos de una Entidad cuyo fin es permitir el normal funcionamiento de esta y/o garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

**PLAN DE PRUEBAS DE RECUPERACIÓN:** Pruebas de recuperación de copias de respaldo programadas con el fin de verificar la consistencia e integridad de las copias de respaldo.

**PLATAFORMA TECNOLÓGICA:** Una plataforma tecnológica es una agrupación de equipamientos técnicos y humanos destinados a ofrecer unos recursos tecnológicos para la realización de las tareas de los usuarios.

**POLÍTICA:** Instrucciones mandatarias que indican la intención y la directriz de la alta gerencia respecto a la operación de la Entidad.

**POLÍTICA DE ESCRITORIO DESPEJADO:** La política de la entidad indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI:** Conjunto de elementos

interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

## 5. POLÍTICAS GENERALES

En Metroplús S.A. La información es un activo de vital importancia, que desempeña un papel fundamental en el día a día de cada funcionario de la organización. Esta información hace parte de la continuidad del negocio, por tal motivo es necesario contar con una cultura de seguridad de forma transversal a todos los procesos tecnológicos de apoyo a la misión y visión general de Metroplús S.A.

Teniendo presente la importancia de la información que se tiene y el papel fundamental que esta desempeña, Metroplús S.A. Implementa un modelo de gestión de seguridad de la información, haciendo uso de herramientas que ayuden a minimizar el impacto de las posibles amenazas a las cuales se exponen. Todo esto permitiendo la continuidad del negocio y ofreciendo una reducción en los costos operativos y financieros.

El proceso de análisis de posibles fuentes que puedan ocasionar fallos relacionados con la disponibilidad, integridad y confidencialidad de la información para luego ser detallados en la Política de Seguridad será ejecutado por el área de TIC, en coordinación con la mesa de ayuda proporcionada por la Plataforma Tecnológica y liderado por la dirección Administrativa, en este caso por el Profesional Especializado de Gestión del Talento Humano y Trámites Administrativos de la entidad, los cuales usarán controles necesarios para llegar a los niveles de protección esperados.

Esta política será revisada con regularidad, con la finalidad de obtener una retroalimentación de parte del área de TIC, y la mesa de ayuda proporcionada por el proveedor de Infraestructura Tecnológica; de tal manera al momento de

evidenciar cambios en los competentes con respecto a la seguridad de la información se plasmarán para su posterior divulgación a los funcionarios de la organización y cumpliendo así un ciclo de mejora continua.

## 5.1 Políticas de Uso General

Dentro de las políticas de Metroplús S.A. es importante la concientización de los usuarios en cuanto al uso adecuado y eficaz de las herramientas de información, que se suministran para el adecuado desarrollo de las funciones asignadas.

En lo sucesivo es el área de TIC, con el apoyo de la mesa de ayuda proporcionada por el proveedor de la Plataforma Tecnológica, quien vela por garantizar que los usuarios hagan uso adecuado y efectivo de la tecnología y que estén conscientes de los riesgos y responsabilidades que conllevan.

El uso inadecuado de la plataforma tecnológica o equipos de cómputo por parte de los usuarios, se reflejaría directamente en costos no previstos, niveles de servicio que no cumplen con las expectativas de los usuarios y con los objetivos y líneas estratégicas de la entidad, exposición a posibles riesgos informáticos, entre otros. De manera alternativa, las operaciones fundamentales podrían verse retrasadas.

5.1.1 El área de TIC en coordinación con la mesa de ayuda proporcionada por el proveedor de la Infraestructura Tecnológica establece las siguientes Políticas de Seguridad de forma general, las cuales representan una visión general en cuanto a la protección de la información.

5.1.2 El área de TIC, en coordinación con la mesa de ayuda, serán los encargados de levantar los posibles riesgos que pueda sufrir la información, documentarlos, promoverlos y actualizarlos a nivel interno de la compañía.

5.1.3 Los activos que componen la infraestructura tecnológica serán inventariados para su fácil ubicación y distinción entre los dispositivos ajenos a la organización.

5.1.4 El área de TIC mediante el uso de controles que ayudarán al uso no autorizado a la información y al acceso a las diferentes plataformas que soportan la infraestructura tecnológica, busca la disminución de los posibles fallos en cuanto a información se refiere.

5.1.5 Todos los funcionarios y/o contratistas y proveedores, son responsables de proteger la información relacionada con su rol específico.

5.1.6 Sólo se permitirá el uso de aplicaciones adquiridas por la organización y avaladas por el área de TIC. En casos extremos el licenciamiento ajeno, a la adquisición de un determinado producto. Este será evaluado para su denegación o posterior implementación.

5.1.7 El área de TIC, en coordinación con la Mesa de Ayuda, realizará periódicamente análisis de posibles fallos y vulnerabilidades de la red de datos de Metroplús S.A.

5.1.8 Cada funcionario de la organización será el responsable de canalizar los requerimientos e incidentes relacionados con la confidencialidad, integridad y disponibilidad de la información.

5.1.9 Nunca suministre información personal a nadie a través de internet.

5.1.10 No intente traspasar las medidas de seguridad instaladas en los equipos de cómputo de la entidad.

5.1.11 Nunca utilice internet para agredir a una persona de alguna forma o para usos indebidos como negocios personales, estudio o actividades no relacionadas con sus funciones.

5.1.12 Proteja su contraseña, use letras mayúsculas, minúsculas, símbolos y/o números y que no sea fácil asociar con su persona. No escriba sus contraseñas en ninguna parte.

5.1.13 Evite tocar la pantalla de los equipos portátiles y los de escritorio, ya que son muy sensibles por el material de que están hechos.

5.1.14 Queda prohibido tener líquidos o alimentos cerca de los equipos de cómputo.

5.1.15 En caso de detectar un funcionamiento anormal o sospechoso en el correo electrónico institucional o en internet, suspenda sus actividades e informe inmediatamente al área de TIC

5.1.16 Las políticas para el adecuado uso de las tecnologías de información de la empresa, son de obligatorio cumplimiento y se pueden ajustar de acuerdo a los requerimientos técnicos que en materia informática se vayan presentando.

5.1.17 Para equipos de cómputo portátiles, siempre se debe usar la guaya de seguridad.

5.1.18 Revisar regularmente la carpeta personal asignada en la Carpeta Compartida (en red) y eliminar los archivos que no se utilicen. Los archivos que sean de uso permanente, se deben ubicar y archivar en la Carpeta Corporativa de cada área.

5.1.19 El área de TIC es la única facultada para administrar y configurar el acceso a los recursos de la plataforma tecnológica en la entidad de acuerdo a la descripción de cargo.

5.1.20 Todo aquel elemento o equipo de hardware retirado de las instalaciones de la entidad debe tener su respectiva orden de salida (formato: DA400-FT-INT-41 Formato autorización salida equipos tecnológicos V1) con la firma del líder de proceso o administrador de infraestructura, la autorización escrita del jefe inmediato.

5.1.21 El manejo de la información y los servicios en la nube están autorizados siempre y cuando se cumpla con los acuerdos de confidencialidad, integridad y disponibilidad, además, que exista un contrato de servicio y el proveedor cumpla con los requerimientos de las normas y legislaciones vigentes.

5.1.22 Se retira y se da de baja aquellos equipos (servidores, desktop o portátiles u otro tipo de hardware) que, por sus características técnicas, software base, soporte han cumplido su vida útil y son punto vulnerable de seguridad.

5.1.23 Se realizan al año dos análisis de vulnerabilidades internas / externas y una prueba de Ethical hacking a todos los servicios y servidores del ambiente de producción de lo cual las vulnerabilidades detectadas se atenderán aquellas que son críticas, altas y medias.

5.1.24 Los equipos de cómputo se asignarán solo a personal vinculado para el uso exclusivo del área o Dirección de la entidad.

5.1.25 Se debe tener mucho cuidado con la manipulación de los activos de información que se impriman, si van a ser reutilizados o reciclados, deben llevar un adecuado proceso de anulación de manera transversal con lo que determine el CAD.

## 5.2 Acuerdos de Confidencialidad

5.2.1 Todos los funcionarios y terceros que laboren dentro y fuera de la organización deben aceptar los acuerdos de confidencialidad expuestos por Metroplús S.A., esto con la finalidad de contar con el uso adecuado de la misma.

5.2.2 En cuanto a los contratistas, estos solo podrán acceder a la información indicada por el área que hace la solicitud de acceso de los mismos. Buscando restringir y/o otorgar de manera precisa el uso de información confidencial y el supervisor tendrá la responsabilidad del manejo que el contratista haga de la información autorizada para su consulta y actividades contractuales. Cabe agregar que el supervisor del contrato, será el único responsable del uso y aplicación de los activos de información y la solicitud debe ser refrendada por este.

## 5.3 Políticas sobre Manejo de Internet y Correo electrónico

Es prioritario para la entidad el fomentar en el usuario un uso racional y prudente del internet. El acceso a éste, se provee como un recurso al usuario autorizado, para apoyar los múltiples objetivos en la conducción de los procesos de Metroplús S.A.

A pesar de que internet y el correo electrónico representan un recurso valioso, también expone tanto a la entidad como al usuario a problemas potenciales de daños y fallas graves en la gestión de la información.

Para ello se enuncian los siguientes puntos, que deben ser conocidos y aplicados por todos los funcionarios (vinculados y contratistas) de la entidad.

5.3.1 El usuario será el responsable de comportamientos inadecuados, abusos no éticos cuando se accede a la red desde las instalaciones de Metroplús S.A.

5.3.2 La persona que no sea empleado de la entidad puede utilizar las conexiones de internet de la Institución, con aprobación de la Dirección Administrativa, únicamente para los propósitos del ente y sólo en las tareas que se hayan asignado a dicho personal.

5.3.3 Utilizar las instalaciones o equipo de cómputo de la entidad de una forma abusiva, no ética o inapropiada en el uso del internet o correo electrónico, no será tolerada y puede ser considerada como causa de una sanción de acuerdo a la ley 1952 de 2019 (Código General Disciplinario).

5.3.4 El usuario debe estar consciente de que el uso de los computadores y servicio de red de la entidad están sujetas a monitoreo. Existe un registro de todos los accesos a internet, por parte de Sistemas de Información. **Algunos ejemplos del uso inapropiado y prohibido** de internet y correo electrónico se mencionan a continuación:

- La descarga de archivos que atenten contra la propiedad intelectual de sus autores. Además de aplicaciones que comprometan la seguridad, integridad y disponibilidad de la información. El uso del canal de internet para el intercambio de información correspondiente a Metroplús S.A. deberá ser informada al jefe inmediato, el cual indicará a la al área de TIC de tal forma que se delegue el tiempo correspondiente para realizar esta labor.
- Intercambio de información confidencial de la organización con previa autorización usando cualquier canal (correo electrónico, sitios web, sitios ftp etc.…)
- El uso de aplicaciones P2P, sitios de mensajería instantánea, los cuales comprometen la información y la infraestructura tecnológica de Metroplús S.A.
- El acceso a sitio de pornografía, hacking, proxys anónimos, o cualquier sitio que atente con las políticas acá establecidas.

- Participar en actividades que causen congestión o interrupción de las redes en actividades de ocio, como escuchar radio, descargar videos, juegos, chatear, etc.
- Revelar o publicitar cualquier información confidencial propiedad de la entidad.
- Presentar opiniones personales como si fueran de la entidad.
- Hacer comentarios, propuestas indecentes o usar lenguaje ofensivo.
- Descargar cualquier software o archivos electrónicos sin tomar las medidas de protección antivirus y software malicioso.

5.3.5 Ninguna información controlada o datos técnicos que no sean del dominio público, deben ser puestos en internet o enviada por correo electrónico a dominio exterior con fines no laborales. En adición toda información confidencial, clasificada o propiedad de la entidad no debe ser compartida con ningún ente externo, excepción hecha solo para casos que autorice expresamente la Gerencia General.

5.3.6 El personal del área de TIC, con el apoyo de la Mesa de Ayuda, suministrada por el proveedor de Infraestructura Tecnológica, serán las encargadas de la revisión periódica del acceso y el consumo de navegación que le dan los usuarios al servicio de internet, esto con la finalidad de ir actualizando las políticas gracias al monitoreo que se le dará al canal.

5.3.7 El tamaño de archivos adjuntos para enviar y recibir por el correo electrónico de la entidad, no sobrepasará los 25 Megabytes por usuario. Se deberá evitar el envío de archivos muy grandes y/o con más de 10 anexos o enviar copias innecesarias. En caso de requerirse el envío de archivos magnéticos muy grandes, se recomienda el uso de la Carpeta “Compartida” y allí en las carpetas “Temporales” de cada usuario, se puede cargar de manera temporal la información en medio magnético que se requiera para la gestión, dando aviso al destinatario que puede tomar los archivos requeridos, procurando mantener con bajo volumen de información dichas carpetas.

La herramienta de Google Drive se debe usar siempre que haya que compartir archivos con peso importante por medio de links y así garantizar que puedan llegar al destinatario.

5.3.8 El área de TIC es el administrador del Correo electrónico, y no podrá interceptar, editar o eliminar ningún mensaje de correo de ningún usuario, salvo autorización expresa de éste o su superior, o en los siguientes casos:

- El usuario haya incurrido en actos ilegales
- Requerimiento expreso de Autoridades Policiales o Judiciales.
- Para identificar o resolver problemas técnicos
- El mensaje compromete el normal funcionamiento del servicio.

5.3.9 El ingreso a internet, correos electrónicos personales y redes sociales, se permite sólo en el horario de almuerzo o fuera del horario de la jornada laboral, esto para evitar congestionar la red en el horario establecido. Solo las personas que laboran en el área de Comunicaciones, están autorizadas por sus labores diarias al ingreso permanente a estas herramientas.

5.3.10 Los usos de las cuentas de correo electrónico deberán ser usadas para desempeñar las funciones asignadas dentro de la entidad.

5.3.11 No se permite el uso del servicio de correo electrónico para el envío de mensajes que no correspondan a las labores indicadas.

5.3.12 Los correos que se encuentren dentro del buzón de cada usuario son propiedad de Metroplús S.A. Esto debido a que los mensajes que se encuentren en la cuenta de correo electrónico hacen referencia a las labores de las funciones indicadas.

5.3.13 En el momento que un funcionario y contratista, persona externa que cuente con una cuenta de correo electrónico no ejerza más labores en Metroplús S.A., la él área de TIC, realizará el cambio de la contraseña, esto si aplica y es solicitado por el Profesional Especializado Talento Humano y Trámites Administrativos (líder del proceso). Además, se podrá realizar la redirección de la cuenta por un periodo de tiempo, para luego bajar la información a medios y contar con dicho histórico.

5.3.14 No está permitido:

- El uso de correos con cadenas que contengan mensajes diferentes a las funciones ejercidas en la organización. Mensajes con contenido que

tengan algún adjunto que pueda perjudicar la información del remitente y comprometer la infraestructura tecnológica.

- El registro de la cuenta de correo en redes sociales y en sitios web en general los cuales son ajenos a las funciones desempeñadas en Metroplús S.A.
- Envío de contenido el cual pueda ocasionar un aumento considerable del almacenamiento del buzón.

5.3.15 El envío de información destinada a un funcionario de la organización, solo podrá ser enviada usando el servicio de correo electrónico correspondiente a Metroplús S.A.

5.3.16 Los mensajes enviados deben respetar los estándares de formato corporativo.

## 5.4 Políticas de uso de los recursos compartidos y carpetas en red.

Todos los usuarios están obligados a acatar los lineamientos para el acceso a la red de la entidad, con el fin de realizar sus operaciones diarias, minimizando el riesgo de llevar a cabo el uso inadecuado o prácticas impropias en dichos recursos.

5.4.1 No se permite que se comparta información directamente desde los equipos. Toda información que se requiera compartir deberá hacerse por medio de las carpetas compartidas en el servidor de archivos. **Recordando que, al ser carpetas temporales, estas son para uso temporal de la información, ésta debe ser utilizada inmediatamente y no permanecer de forma indefinida almacenada. Deben ser depuradas mínimo cada quince días para evitar el exceso de almacenamiento. De no hacerlo en ese lapso de tiempo la información se borrará automáticamente.**

5.4.2 Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través del área de TIC.

5.4.3 Sólo podrá hacerse uso de los recursos o carpetas de red de la entidad desde los equipos a cargo de Metroplús S.A., salvo en los casos que se presente la modalidad de trabajo en casa y se deberá utilizar la VPN y sólo para servidores públicos.

5.4.4 El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta. El tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado). Cabe agregar que el control total de las carpetas de red sólo será para los servidores públicos de la entidad; contratistas y terceros sólo podrán tener permisos para visualizar las carpetas y para lectura.

5.4.5 En caso de que excepcionalmente se requiera que un tercero o contratista tenga otros tipos de permisos sobre las carpetas de red, será el supervisor del contrato el directo responsable del control al manejo dado a la información; el compromiso será por escrito y el director Administrativo o quien haga sus veces, será quien apruebe dicha situación, dicha aprobación debe ser por escrito.

5.4.6 Existirá en la carpeta compartida, una subcarpeta que se denominará “Contratistas Metroplús S.A.”, donde tendrán los contratistas de la entidad su carpeta, que tendrá su nombre y la extensión contratista.

5.4.7 Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo. Cabe agregar que solo podrá tenerse activa en la carpeta esa información máximo quince días.

5.4.8 El acceso a carpetas compartidas debe limitarse a los usuarios que las necesitan.

5.4.9 No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

5.4.10 No se permite que los funcionarios conecten impresoras personales en las instalaciones de la entidad. Solo se autoriza el uso de las impresoras ubicadas en los pisos de la empresa. Tampoco se permite que se conecten accesorios como teclados, pantallas, mouse, etc., que no sean propiedad de Metroplús S.A.

5.4.11 Todos los archivos almacenados en las computadoras y en los directorios personales en la red, son propiedad de Metroplús S.A y no de los usuarios. Por lo tanto, solo deben contener archivos con información relacionada con la actividad propia de la entidad y de sus funciones diarias.

5.4.12 Los usuarios deben ser conscientes que, en caso de retiro de la institución, sea este voluntario o involuntario, deberán entregar toda la información contenida en sus equipos. En el formato de “Paz Y Salvos De Retiro De Personal” (código DA410-FT-GTH-55), se diligencian los ítems relacionados con equipos informáticos e información con el apoyo de la Asistente Administrativa, quien recibe este formato e informa al responsable en el área de TIC sobre la novedad.

5.4.13 Para respaldos o resguardos de información que se pidan al área de TIC, solo se ejecutará sobre información relacionada a sus labores en la institución, por lo tanto, queda excluida toda información que no sea de carácter laboral, por ejemplo: información personal, música, fotos, videos, entre otras.

5.4.14 Los archivos almacenados en los recursos y servicios de red pueden convertirse en evidencia para procedimientos legales, por lo que todo usuario autoriza a la entidad para la revisión de cualquiera de ellos, así como el uso de la información para diversos propósitos y la divulgación de éstos a terceros (Control Interno, Entes de Control, algún tercero que apoye a la entidad en algún procedimiento legal, entre otros).

5.4.15 La información que genere cada funcionario y que se almacene en los equipos de cómputo o en el correo electrónico institucional, se considera como parte de la información de Metroplús S.A. que se puede revisar y auditar en cualquier momento por los órganos de control que lo requieran.

5.4.16 No se debe permitir el acceso a la infraestructura de la red sea alámbrica o inalámbrica, a los equipos de cómputo a personas u organizaciones ajenas a la entidad sin autorización expresa de la Dirección Administrativa. Solo se conectarán equipos a la red de datos bajo la autorización de la Dirección Administrativa. En este caso, la entidad no se responsabiliza por daños (Físicos/Lógicos) que ocurran en equipos de cómputo y cualquier otro recurso tecnológico que no sea propiedad de Metroplús S.A. Cabe agregar

que en casos excepcionales se hará bajo la responsabilidad expresa escrita del supervisor del contrato del tratamiento que el contratista tenga con el activo de información.

5.4.17 El usuario debe aplicar los estándares normales de comunicación, el servidor de archivos deberá ser usado únicamente para compartir información laboral, con lenguaje apropiado, sin utilizar expresiones anónimas en contra de algún individuo o grupo que contenga material ofensivo.

5.4.18 El material explícitamente sexual, queda expresamente prohibido, por lo que quien se encuentre usando, enviando o archivando este tipo de información, será sujeto a una acción disciplinaria determinada por la Dirección Administrativa.

5.4.19 No deberán existir archivos con formatos como juegos, videos, archivos con contenido pornográfico, música, entre otros, en las carpetas de red y en los equipos locales ya que serán borrados y para el caso de respaldos, éstos no se considerarán ya que no es información para uso laboral. Salvo por las personas autorizadas por Sistemas de Información, justificadas por sus superiores cuyas funciones laborales impliquen el uso de dichos archivos.

5.4.20 Las carpetas de red o la información que se comparta en red es responsabilidad de cada usuario de la Entidad y la deben mantener depurada. No se debe tener información crítica o confidencial en dichas carpetas. La información contenida en las carpetas compartidas del servidor, se puede borrar por parte del personal de Sistemas de Información en caso de saturarse de información.

**Nomenclatura de Archivos y Carpetas.**

5.4.21 Tener en cuenta que los nombres extensos en los archivos, pueden generar demoras o problemas en su recepción o envío por internet y por el correo electrónico, es por esto que se sugiere que se usen nombres cortos y explicativos del tipo de archivo, además tener en cuenta este punto para

cuando se hace la conversión a archivos en formato PDF o imagen electrónica.

## 5.5. Políticas de Firewall

5.5.1. Metroplús S.A., tiene dispositivos de seguridad perimetral (Firewall) en todas las sedes donde tiene infraestructura y controla el tráfico y seguridad de la información.

5.1.2. Al realizar cambios o actualizaciones en el firewall se realiza un Backup en un medio externo con el fin de garantizar la integridad e inmediato retorno a un escenario funcional.
5.2.3. Se debe llevar un registro de todo cambio realizado en la consola de control perimetral.
5.2.4. El intercambio de información con entidades se hace a través de una conexión VPN punto a punto cumpliendo con los requerimientos de cifrado y seguridad que exige la norma y legislación vigente.
5.2.5. Para todos los equipos de escritorio de la entidad se tiene habilitado el servicio de firewall local de acuerdo con las políticas de la herramienta de antimalware.
5.2.6. Para todo firewall nuevo que se conecte a la plataforma tecnológica se incluye en los diagramas de red, guías de hardening y configuración. La última versión liberada de firmware está aplicada.
5.2.7. Por parte del área de TIC, se realizará auditorías en los activos de criticidad alta cada 6 meses.

## 5.5 Política de Uso de contraseñas y accesos a los servicios de Sistemas de Información.

5.5.1 La creación de las cuentas para el acceso a los equipos y la red de los empleados serán solicitadas por la Dirección Administrativa al área de TIC, esta debe contener nombre completo, área a la que pertenece y ubicación.
5.5.2 Para la “clave” y nombre de usuario, deberá tener en cuenta lo siguiente:

- Las “claves” de usuario deben ser alfanuméricas, contener caracteres especiales y una longitud no menor a 8 (ocho) sin utilizar espacios en blanco.
- Deben contener tanto caracteres alfabéticos como numéricos.
- No deben ser fácilmente descifrados, ni deben revelarse bajo ninguna circunstancia.
- No se deben utilizar “claves” previamente utilizadas.
- El nombre de usuario y la “clave” deben ser diferentes entre sí.
- No se deben utilizar claves con información fácilmente identificable como, fecha de cumpleaños, Nombre de la mascota, nombres de familiares y apellidos, números de identificación, y/o demás información personal evidente

5.5.3 El uso de esta cuenta es de uso personal e intransferible.

5.5.4 La asignación se realizará de tal forma que el usuario realice el cambio de contraseña luego del primer ingreso.

5.5.5 Los recursos de la red están asignados según el privilegio otorgado para desempeñar sus labores sobre los mismos.

5.5.6 No se deben dejar nombres de usuario y “claves” escritos en lugares donde puedan ser vistos o tomados por terceros (por ejemplo, en la carpeta del escritorio, pantalla del equipo, etc.).

5.5.7 No se debe enviar el usuario y contraseña por mail o por fax o decírselo a alguien.

5.5.8 Cada usuario es responsable por la actividad realizada bajo su cuenta personal de red.

5.5.9 Nadie debe intentar acceder a la cuenta de otra persona.

5.5.10 Los usuarios no deben dejar desatendidas las estaciones de trabajo. Todo funcionario es responsable de desactivar las aplicaciones (cerrarlas) de ser necesario, cada vez que se ausente de su puesto de trabajo, y dejarla bloqueada con contraseña.

5.5.11 Los cambios de contraseña pueden solicitarse al área de TIC, las contraseñas deben protegerse en todo momento y deben cambiarse con cierta frecuencia de acuerdo con los procedimientos actuales cada 30 días.

5.5.12 Está prohibido prestar el usuario y contraseña personal, para fines de cualquier tipo, en caso que el funcionario se encuentre en vacaciones, incapacitado o en licencia, la Dirección Administrativa autorizará el acceso a la red interna, cuenta de correo electrónico institucional y equipo de cómputo personal de estas personas, solo para fines de dar continuidad a los procesos o en caso de ser requerido.

5.5.13 Debe mantenerse activo el detector de intrusos al equipo de cómputo, restringiendo el número de intentos de ingresos fallidos a tres. La reactivación del código de usuario debe ser solicitada al área de TIC.

5.5.14 El área de TIC es responsable de dejar deshabilitados los derechos de acceso de aquellos funcionarios que deban ausentarse de sus labores por concepto de vacaciones, incapacidad, permisos y otros. Una vez sea informado por el Grupo de Desarrollo Humano, el jefe respectivo autorizará si así lo requiere los nuevos accesos del personal de reemplazo de los privilegios que fueron suspendidos temporalmente hasta el regreso del titular.

5.5.15 La mesa de ayuda de la empresa proveedora de la infraestructura tecnológica, será autorizada por el área de TIC, a inactivar las cuentas de los usuarios en el directorio activo, que solicite el Profesional Especializado Talento Humano y Trámites Administrativos o Profesional Universitario III Administrativa, ninguna cuenta deberá ser eliminada.

5.5.16 Se debe mantener en un sobre sellado y bajo custodia la “clave” que posea todos los privilegios del Administrador de la Red, Administrador de Base Datos u otros y dispositivos de Telecomunicaciones, para ser utilizado solamente en caso de emergencia. La “clave” debe ser cambiada periódicamente mínimo una vez al año o en caso de rotación del personal del área de TIC.

5.5.17 Los externos con autorizaciones podrán acceder remotamente a los sistemas de Metroplús S.A. Esto se realizará con un acompañamiento del área de TIC. En caso tal que sea necesario realizar la instalación, modificación u otra actividad administrativa dentro del sistema en cuestión, el ingreso de las credenciales las digitará el personal encargado del área de TIC.

5.5.18 Únicamente las personas permitidas por la organización podrán acceder a la red inalámbrica corporativa y la red inalámbrica llamada "*Invitados"*.

5.5.19 Para la asignación de cuentas de correo electrónico, que se hace al personal nuevo, se deben nombrar con el primer nombre y primer apellido, en caso de existir un homónimo, se asignará con el segundo nombre y primer apellido.

## 5.6 Política de Utilización de software estándar o autorizado.

El uso de software sin licencia pone en peligro a la entidad de sufrir repercusiones de carácter legal que incluyen allanamiento, incautación, sanciones económicas, así como publicidad negativa. El uso de software no autorizado puede obstaculizar la operación del software autorizado e incluso introducir virus, además que el software innecesario desperdicia los recursos de la entidad en detrimento del patrimonio.

5.6.1 El usuario únicamente podrá utilizar en sus labores diarias el software de aplicaciones autorizado previamente e instalado en cada equipo asignado solo por el personal del área de TIC.

5.6.2 El área de TIC, tiene la facultad de revisar y comprobar periódicamente el software instalado en los equipos de acuerdo al inventario de software con licencia, lo cual se realizará al menos una vez al año.

5.6.3 Al usuario que se le encuentre un software no autorizado (como software de programas, protectores de pantalla, tapices o juegos, entre otros) le serán removidos de sus equipos y si existe reincidencia, serán sancionados con una acción disciplinaria, determinada por la Dirección Administrativa.

5.6.4 Todo usuario que requiera de la instalación de un software especial, deberá solicitarlo a Sistemas de Información, proporcionándole su licencia de uso o en su caso indicar que tipo de software requiere, anexando la debida autorización por escrito del coordinador o responsable de área que permita su instalación por parte del personal de Sistemas de Información. Como entidad pública no podemos hacer uso de software que no cuente con licencia vigente, si existe la necesidad de utilizar cualquier software para su trabajo se les pide que soliciten las licencias correspondientes. Atendiendo a la suficiencia presupuestal, se evaluará la conveniencia de adquirir dicho

software, así como sus licencias y la importancia de la adquisición de la misma.

5.6.5 Para todo software de libre distribución o de código abierto que no implica costo en su adquisición o licencia, también se deberá solicitar la previa autorización por Sistemas de Información y superiores con la justificación debida, y que la aplicación no interfiere con sus labores ni con el rendimiento del equipo o favorece a las actividades del usuario.

5.6.6 El Director de cada área, es el responsable de determinar quién debe tener acceso y que privilegios se otorgan para las aplicaciones de la entidad (por ejemplo, en los sistemas financieros la Dirección Financiera será responsable de asignar permisos y privilegios a los usuarios que utilicen estos sistemas por la importancia de la información que se manejan en los mismos, en la coordinación de Comunicaciones es la responsable directa de la administración de la página web, administración de la Intranet y demás contenido almacenado en la Web de Internet, el CAD es responsable de administrar el sistema documental y cualquier sistema en general). Al determinar los privilegios de acceso de un usuario, el responsable debe asegurarse de que se conserve la división de obligaciones y que se cumplan con los requerimientos laborales, así como la fecha de expiración de esos privilegios.

5.6.7 Si un usuario necesita cambios en su perfil, deberá solicitarlo y justificar mediante e-mail a la persona responsable del sistema de información, la cual asignará el perfil y responderá con un e-mail. De igual manera para los procedimientos de cambios de claves se procederá a hacer solicitud con memorando al responsable respectivo.

5.6.8 Las estaciones de trabajo, redes y otros medios que pueden ser afectados por virus informáticos, deben contar con software antivirus, el cual debe ser actualizado periódicamente y bajo una política única de actualización global del Servidor de Antivirus.

5.6.9 El área de TIC, será la encargada de realizar el despliegue de las actualizaciones sobre los diferentes programas. Esto incluye actualizaciones

del Sistema Operativo. Periódicamente se evaluarán las actualizaciones lanzadas por los proveedores para su posterior instalación.

## 5.7 Políticas sobre Uso de Computadores de Oficina y Portátiles

El usuario tiene la obligación de hacer uso adecuado de los equipos de cómputo de la entidad; cualquier daño en el hardware (equipo físico) o software (sistema operativo o programas) de los equipos deberá ser notificado al área de TIC, para realizar el diagnóstico y hacer la reparación o uso de la garantía con el proveedor.
Es responsabilidad de los usuarios reportar el hurto del equipo o componentes, este debe estar acompañado del denuncio, el cual es emitido por la Policía Nacional.

5.7.1 Ningún usuario, sin la debida autorización de área de TIC, puede conectar dispositivos externos al equipo de cómputo; de hacerlo sin autorización, todo daño que le suceda al hardware o al software será único responsable.

5.7.2 Si en el diagnóstico se deduce que el daño es por mal uso, negligencia o descuido, el usuario deberá pagar las reparaciones o la compra del bien. El desconocimiento del uso correcto tampoco será causa para justificar un daño.

5.7.3 Es responsabilidad del usuario, cuidar y mantener los equipos de cómputo bajo su resguardo. Está prohibido fumar, tomar bebidas o alimentos cuando esté haciendo uso de cualquier equipo electrónico de la institución (computadoras, impresoras, proyectores, teléfonos, etc.) y puede ser considerada como causa de una sanción de acuerdo a la ley 1952 de 2019 (Nuevo Código Disciplinario).

5.7.4 Está estrictamente prohibido el intercambio de computadoras, accesorios o aditamentos entre usuarios sin previo aviso y autorización de Sistemas de Información o Dirección Administrativa.

5.7.5 Las impresoras y escáneres de la entidad no deben ser usados para fines personales (imprimir trabajos personales y de cualquier índole, utilizar los escáneres como fotocopiadoras, entre otras). Igualmente se debe tener cuidado en no alimentar estos equipos con papel que contenga ganchos de cosedora, que pueden dañarlo. En caso de determinarse que un daño es

producido por mal uso, la Dirección Administrativa determinará la sanción disciplinaria y costo.

5.7.6 Hacer un buen uso de los equipos de cómputo de la entidad hace parte de las responsabilidades del funcionario, quien al finalizar la jornada laboral debe apagar completamente el monitor, disco duro y demás equipos a cargo como impresoras, escáner, entre otros. Así se puede evitar que estos equipos sufran fallas eléctricas, cortocircuitos o de otro tipo durante las noches. El servidor de la empresa, debe ser manipulado solo por personal autorizado del área de TIC.

5.7.7 Para evitar el daño de los adaptadores de corriente se recomienda evitar golpearlos, desconectarlos con cuidado, no tirar del cable y enrollarlo de manera inadecuada; además de no cambiarlos por los de otra computadora, ya que de ser necesario tramitar alguna garantía esta no será válida si los números de serie del computador y adaptador no corresponden.

5.7.8 No se deben guardar los equipos portátiles encendidos en los maletines (computador portátil), al hacerlo se pueden dañar dispositivos internos de estos equipos. De presentarse un daño, la Dirección Administrativa determinará la responsabilidad y el costo del daño para que el responsable asuma con los gastos.

5.7.9 Si al recibir el computador, le faltan accesorios o no funcionan correctamente, se debe informar inmediatamente al responsable del área de TIC, es responsabilidad de la persona que hace el préstamo revisar que tiene todos los accesorios como cables, mouse y adaptadores.

5.7.10 El área de TIC, es el encargado de Control de Activos deberá tener un registro de todos los equipos propiedad de Metroplús S.A. (Propios y Arrendados) y debidamente ingresados en el sistema de inventarios de OCS, este deberá contener el nombre del funcionario que tiene a cargo el equipo o recurso tecnológico en el inventario fiscal debidamente actualizado.

5.7.11 Todos los equipos tecnológicos deben ser objeto de mantenimiento preventivo, de conformidad con un cronograma preestablecido por el área de TIC (se recomienda que sea uno o dos en el año, dependiendo las condiciones de ambiente donde esté ubicado el equipo).

5.7.12 Se debe mantener el equipo informático en un lugar limpio y sin humedad.

5.7.13 Para prevenir la pérdida de información, daño o el compromiso de los activos de información y la interrupción de las actividades, los equipos deben estar conectados a la toma regulada destinada para tal fin.

5.7.14 Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su actividad. Todos los colaboradores, consultores, contratistas, terceras partes, deben bloquear la sesión al alejarse de su computador.

5.7.15 Todos los equipos en arriendo que sean retirados por el contratista deben estar debidamente formateados, para evitar la fuga de información.

5.7.16 Los equipos de cómputo (fijo y portátil), siempre deben ir conectados a los reguladores.

**Traslado de equipos.**

5.7.17 Siempre que transporte el equipo portátil colóquelo dentro de su maletín o en los morrales corporativos, que lo protegen de golpes ligeros. Asegúrese que tiene todos los accesorios como cables de conexión y mouse, si falta algún accesorio, informe oportunamente a la persona encargada.

5.7.18 Los equipos portátiles y demás equipos de la entidad no deben ser retirados sin permiso respectivo por la persona encargada y que controla el préstamo de dichos activos, procurar al máximo que no se conserven estos equipos los fines de semana en préstamo para minimizar el riesgo de pérdida, robo o daño.

**Autorización salida de equipos tecnológicos**

5.7.19 Cuando la entidad tenga jornada laboral in house, se debe autorizar a todos los funcionarios a retirar de la entidad los equipos portátiles, pues son necesarios para el desarrollo de sus actividades habituales. Cabe agregar que para poder sacarlo; cada empleado debe diligenciar el formato DA400-FT-INT-41 Formato de autorización salida de equipos tecnológicos V1 y entregarlo al área de TIC, que es el área encargada del inventario de los elementos tecnológicos.

5.7.20 Si la entidad está trabajando con la jornada laboral normal, la salida de equipos sólo procederá en casos excepcionales considerados por el jefe inmediato; y se deberá seguir la siguiente ruta: se debe enviar un correo electrónico al jefe inmediato solicitando autorización con copia al encargado del área de TICS y diligenciar el formato DA400-FT-INT-41 Formato de autorización salida de equipos tecnológicos V1. Dicha autorización debe ser refrendada por el encargado del área de TICS, este último será el encargado de aprobar o desaprobar dicha solicitud.

## 5.8 Políticas sobre el ingreso y uso de computadores de escritorio y portátiles propiedad del contratista

5.8.1 El software instalado en el equipo de cómputo deberá poseer la licencia correspondiente y en caso de ser requerido deberá sustentar la legalidad del mismo.

5.8.2 El contratista debe garantizar que el sistema de cómputo cuenta con un software antivirus y control de malware y con las últimas actualizaciones instaladas.

5.8.3 Realizar un escaneo y limpieza de virus y malware al sistema de cómputo previo a la conexión del equipo a la red de Metroplús S.A.

5.8.4 La información directamente relacionada con Metroplús S.A y sus diferentes actividades, deberá residir en los servidores de almacenamiento que provee la organización y solo podrá acceder a la información autorizada por la Dirección Administrativa y el supervisor del contrato debe hacerse responsable del control al tratamiento que el contratista haga con la información, dicho compromiso debe ser por escrito.

5.8.5 En caso de que se requiera extraer información de Metroplús S.A., este proceso deberá ser autorizado de manera escrita por la Dirección Administrativa y/o el jefe del área donde se especifique el contenido y el objetivo de la salida de la información.

## 5.9 Política de Respaldos de la información o “Backups”.

Las políticas sobre los respaldos de información o “Backups”, se establecen para sensibilizar al usuario de los riesgos que existen de la pérdida de la misma, debe tener la conciencia sobre el valor que tiene la información y los datos para la entidad, ya que representa el trabajo diario y el conocimiento de la entidad. Para ello debe tener en cuenta que:

5.9.1 El área de TIC con el apoyo de la Mesa de Ayuda, suministrada por el proveedor de la Plataforma Tecnológica; está en la obligación de asegurar que la información clasificada contenida en la plataforma tecnológica de la compañía, encontrada en los diferentes Servidores que soportan las aplicaciones y ofrecen el rol de Servidor de Archivos sea periódicamente resguardada mediante uso de herramientas y prácticas que garanticen la disponibilidad, integridad y seguridad de los datos.

5.9.2 Debe crearse una programación sistemática de los procesos de respaldo (diarios, semanales, mensuales y anuales), además se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.

5.9.3 Se debe generar una copia de todos los respaldos, los cuales se custodiarán en un sitio alterno, que cumpla con las características y protección ambiental similares al sitio principal.

5.9.4 Los equipos y los medios usados para el respaldo deben ser sometidos a un mantenimiento preventivo por parte del proveedor (al menos dos veces al año) que asegure las condiciones adecuadas de funcionamiento.

5.9.5 El área de TIC, ha asignado a cada perfil de usuario de dominio una unidad de red en la cual almacenarán información de carácter estrictamente laboral, no se podrá almacenar fotos, música, videos e información personal.

5.9.6 Será responsabilidad de cada funcionario de Metroplús S.A., realizar el respaldo de su información de su estación de trabajo.

5.9.7 No se realizarán respaldos o “backups” de información a las carpetas personales, escritorios u otros, la información de cada persona que se debe respaldar, debe reposar en la carpeta de usuario ubicada en la unidad C:

### 5.10 Política de Manejo del Antivirus.

5.10.1 Es obligación del usuario establecer la disciplina de revisar los archivos, correos y dispositivos para detectar y eliminar virus y evitar el contagio de equipos y la difusión de los mismos. Se puede solicitar al área de TIC, el apoyo para realizar esta actividad.

5.10.2 Nunca se deben abrir mensajes, archivos o macros adjuntos de un correo con procedencia desconocida, sospechosa o fuente no confiable.

Son obligaciones del usuario de la red de Metroplús S.A.:

- Borrar el spam, cadenas y cualquier correo del mismo. No realizar reenvío de los mismos (Ver Circular de la Alcaldía de Medellín “Secretaría Privada No. 005 de 2010”).
- Nunca descargar archivos de sitios desconocidos o fuentes sospechosas.
- Siempre revisar con el programa antivirus sus unidades USB, discos removibles o memorias flash **antes de usarlas**.
- Respaldar información crítica en forma regular y almacenar la información en un lugar seguro.
- Si detecta alguna contingencia con virus, desconecte su equipo del cable de red y reporte directamente al área de TIC.

El servidor de la entidad, realiza periódicamente la ejecución del antivirus para todos los computadores.

### 5.11 Política de los Mantenimiento preventivo y correctivo de los equipos de cómputo

5.11.1 La entidad recibe 2 veces al año el servicio de mantenimiento preventivo de todos sus computadores.

5.11.2 El usuario no deberá limpiar partes delicadas del computador, para ello debe solicitar mantenimiento al área de TIC en caso de necesitarlas.

5.11.3 La programación del mantenimiento preventivo de equipos de cómputo, será realizada e implementada por el área de TIC con el apoyo de la Mesa de Ayuda proporcionada por el proveedor de la Plataforma Tecnológica, quienes con suficiente antelación lo informarán a los usuarios que serán atendidos.

5.11.4 Para el mantenimiento correctivo de los equipos, cuando se presente algún daño en los programas, bases de datos, sistemas de información y computadores, se reportan inmediatamente al área de TIC, quien escalará a la mesa de ayuda proporcionada por el proveedor de la Plataforma Tecnológica, quienes atenderán el caso a la mayor brevedad informando al usuario las novedades encontradas y acciones de mejora ejecutadas.

### 5.12 Política de Acceso Físico

5.12.1 Se dispone de un control restringido al centro de cómputo, el cual solo podrá acceder al personal del área de TIC, esto debido a que en esta zona se ubican equipos sensibles que soportan el sistema de información de toda la entidad.

5.12.2 En caso tal que sea necesario por parte de personas ajenas al área de TIC, el ingreso al centro de cómputo, ya sea por alguna labor administrativa que sea solicitada por el área o por parte de la administración, personal de Sistemas realizará el acompañamiento y será la encargada de realizar el controlar el acceso.

### 5.13 Política de ubicación y protección de dispositivos

Los dispositivos que hacen parte de Metroplús S.A. y soportan la infraestructura tecnológica son:

5.13.1 Servidores, equipos activos, dispositivo de seguridad, cableado estructurado, UPS, aires acondicionados, plantas telefónicas, dispositivos de almacenamientos, deberán ser ubicados adecuadamente, de tal manera que no sean expuestos a accidentes o a amenazas potenciales, tales como polvo, pérdida, agua, vibración, entre otros.

5.13.2 En este sitio no se permite el ingreso de alimentos los cuales podrán ocasionar algún daño sobre los dispositivos.

### 5.14 Política de pérdida del dispositivo

5.14.1 En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la entidad, se debe reportar la pérdida al área de las TIC lo más pronto posible y realizar el procedimiento de gestión de incidente de seguridad, este debe estar acompañado de la denuncia ante las autoridades públicas como (Policía o Fiscalía).

5.14.2 El empleado y contratista que tiene la necesidad de utilizar el recurso USB o la unidad CD/DVD debe hacer la solicitud mediante correo electrónico a la dirección Administrativa a través del soporte técnico de la entidad, al correo soporte.sistemas@metroplus.gov.co, indicando la justificación de la necesidad.

5.14.3 El técnico de soporte deberá registrar y escalar la solicitud al área administrativa para obtener la autorización o denegación el recurso solicitado.

### 5.15 Monitoreo y Verificación

El área de TIC con apoyo de la mesa de ayuda suministrada por el proveedor de la Plataforma Tecnológica, monitorea los recursos, servicios de red, servicio de internet, el sitio Web de la entidad lo monitorea el área de Comunicaciones por medio de su administrador de la página web.

Revisando el tráfico de las operaciones del servidor con cierta continuidad, con el objetivo de tener una mejor administración de los recursos y vigilar patrones que garanticen el buen funcionamiento de los mismos.

El monitoreo comprende:

- Congestión extrema de la red, relacionada con el tráfico de información dentro de la red.

- Operación anormal de los servicios de red.
- Accesos no autorizados a los servicios de red.
- Monitoreo de las colas de impresión (cancelación, reanudación, pausa a los trabajos de impresión).
- Monitoreo de cuentas de acceso activas.
- Auditorías a los recursos de red (equipos de cómputo), para la detección de software no autorizado, detección de virus, etc.
- Virus dentro de los servicios de red.
- Habilitación de cuentas de red bloqueadas.
- Escaneo de los equipos de los usuarios, para evitar virus y software peligroso.
- Monitoreo del servicio de internet.

Y cualquier otra actividad que sea necesaria para mantener la integridad de los equipos y la información.

Además, es necesario crear y mantener una cultura de la seguridad informática y de buen uso de las herramientas de cómputo, reforzando aquellas políticas que sean de uso más crítico y que ameriten un acompañamiento continuo por parte del área de TIC.
Se capacitará al usuario que ingrese a la entidad, en el uso de las políticas de seguridad informática más relevantes.

## 5.15. Política de Áreas Seguras

5.15.1. Se establece como áreas seguras aquellas ubicaciones sobre las cuales existen mecanismos de control que garanticen la seguridad de la información solo a personal autorizado. Estas son:

- Área de oficina
- Data Center Local
- Racks piso 4 y 5

5.15.2. Para él Data Center se tiene establecido contractualmente las condiciones que contemplan las políticas y procedimientos de seguridad.
5.15.3. Establecer un formato para el ingreso al Data Center, cuando se trate del ingreso de algún proveedor, se debe pedir la orden de servicio y poner esa información en el campo de observaciones, la orden de servicio debe llevar la actividad a realizar y la hora de ingreso y salida.

### 5.16. Políticas de Backup

5.16.1. Los funcionarios son responsables de realizar y actualizar los respaldos de la información que tiene en el equipo asignado mínimo cada 8 días.
5.16.2. La restauración del Backup full de las bases de datos de producción y de los servidores definidos como críticos, se debe realizar una semanal, una mensual y una semestral en la herramienta de Backup de la entidad.
5.16.3. El área de TIC garantiza los respaldos de información que reposa en los ambientes productivos, los que se entregarán en custodia a la Dirección Financiera bajo los RTO y RPO definidos en los acuerdos contractuales. De esta custodia se diligenciará en cada entrega el formato DA400-FT-INT-39 Formato de entrega de Backups (custodia) V1
5.16.4. Se realiza un Backup diario full de las bases de datos en la herramienta de Backup de la entidad.
5.16.5. Para el retiro de un funcionario de la entidad se realiza un Backup de la información por parte del área de TIC tan pronto se reciba el portátil o equipo asignado por la entidad y también de su cuenta de correo electrónico y de las carpetas compartidas. Además, se realiza la cancelación de la cuenta en el directorio activo.

### 5.17. Política de acceso físico

5.17.1. El acceso al Data Center está restringido únicamente al personal autorizado y bajo la supervisión del área de TIC con previa aprobación.

5.17.2. Para la autorización de acceso al Data Center, por parte proveedores se diligencia el formato de ingreso y este debe estar autorizada y tramitada por el área de TIC, verificando la orden de servicio y la hora de ingreso y salida.
5.17.3. Para el acceso al Data Center se tiene dos copias, las cuales están a cargo del área de TIC, una la portará el Técnico de Soporte y Sistemas y la otra estará en custodia del Profesional Universitario Gestión TIC y Servicios Administrativos.
5.17.4. Para los visitantes, el funcionario que autoriza su ingreso lo acompaña de manera permanente mientras permanezca dentro de las instalaciones de la entidad.
5.17.5. Para la transferencia de información se utiliza sitio seguro SFTP asignando un usuario y contraseña.
5.17.6. Para la entrega de información, se establecen mecanismos de protección de la información como puertos seguros, cifrado y la contraseña se entrega por otro medio.

### 5.18. Política de acceso remoto

5.18.1. El acceso remoto a los servidores críticos y bases de datos, se realizan con la debida autorización del Profesional Universitario Gestión TIC y Servicios Administrativos.
5.18.2. Se establece que el tiempo de desconexión por inactividad de la sesión es de 10 minutos.
5.18.3. El Profesional Universitario Gestión TIC y Servicios Administrativos, autoriza los accesos remotos de los empleados y proveedores.
5.18.4. Está prohibido copiar, mover o almacenar información de las bases de datos de los servidores cuando se acceda mediante tecnologías de acceso remoto.

### 5.19. Política de Transición de IPv4 a IPv6

5.19.1. Debe ser estructurado con esquemas de seguridad y privacidad de la información, de las cuales debe cumplir con las políticas de confidencialidad, disponibilidad e integridad.
5.19.2. Debe prepararse un rollback, para los casos de indisponibilidad en los servicios.

5.19.3. Se debe revisar los procesos de transición hacia el nuevo protocolo, analizando los niveles de impacto en los servicios como:

- Directorio Activo
- DNS
- Correo Electrónico
- Host – DHCP
- Proxy
- Aplicaciones
- Web
- Gestión y Monitoreo

5.19.4. Mantener los mismos nombres de servicios utilizados sobre la red tanto para IPv4 como para IPv6.
15.19.5. No usar direcciones IPv6 literales en el desarrollo del software y en el uso de librerías de software.
15.19.6. Analizar y documentar los riesgos asociados a la transición de IPv4 a IPv6.

**15.20. Políticas de escritorio limpio**

15.20.1. Ejecutar el bloqueo de pantalla siempre que el responsable o usuario del equipo se ausente de la terminal, ejecutando la combinación de teclas Windows () + L
15.20.2. Cerrar sesiones de usuario cuando no se requiera los servicios del equipo durante tiempos superiores a 3 minutos.
15.20.3. Ejecutar el procedimiento de clasificación, etiquetado y manejo de la información de forma segura y ordenada en rutas de acceso recordables.
15.20.4. En la pantalla no debe permanecer ningún icono, acceso directo o archivo, esta debe estar completamente despejada.
15.20.5. Para el personal operativo en la pantalla solo deben permanecer los iconos de acceso directo a las diferentes herramientas de gestión de la solución, no deben permanecer archivos digitales de ningún tipo.

## 15.21. Política de seguridad en la nube

15.21.1. Realizar monitoreo a los logs de transferencia de datos hacia la nube.
15.21.2. Implementar controles de criptografía para la transferencia de información.
15.21.3. Proteger los volúmenes de su exposición a un clonado mediante Snapshot.
15.21.4. Realizar Backup de la información que se envía hacia la nube

## 15.22. Política de Gestión del Incidente

15.22.1. Se definen roles y responsabilidades dentro de la entidad para evaluar los riesgos y así mantener la operación, la continuidad y la disponibilidad del servicio.
15.22.2. Gestionar los eventos de seguridad de la información para detectar e identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
15.22.3. Definir de manera oportuna los eventos de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
15.22.4. Asegurar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Con el fin de mejorar el esquema global de la gestión de incidentes de seguridad de la información.
15.22.5. Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
15.22.6. Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
15.22.7. Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.
15.22.8. Informar de forma completa e inmediata al ColCert (Grupo de respuesta a emergencias cibernéticas de Colombia), la existencia de un potencial incidente de seguridad informática que afecte a activos de información críticos del Estado.

## 15.23. Política de Gestión del Riesgo

15.23.1. Se deben identificar riesgos para todos los procesos y activos que conforman la Metroplús S.A.
15.23.2. Se debe realizar la verificación y actualización de los riesgos identificados, por lo menos una vez al año, cada vez que se identifique un nuevo riesgo o al presentarse un accidente fatal o grave.
15.23.3. Es responsabilidad de los directores de procesos, así como de su personal a cargo realizar la identificación y verificación de riesgos con el apoyo de las áreas de seguridad y de aseguramiento de la información.
15.23.4. Teniendo en cuenta la identificación y priorización de riesgos realizada, se debe gestionar primero los riesgos en nivel alto, seguidos del nivel medio y Nivel bajo.
15.23.5. Para los riesgos identificados con nivel alto, seguidos del nivel medio la decisión de mitigar, aceptar o transferir el riesgo estará a cargo del comité directivo de la entidad.

## 6. SANCIONES A LAS VIOLACIONES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El área de TIC, solicitará la publicación en la Intranet del documento Manual de Políticas de Seguridad de la Información, se debe socializar su contenido y hará cumplir su alcance.

El desconocimiento de la política de seguridad de la información de Metroplús S.A., por parte de funcionarios, contratistas y terceros puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones le corresponden a la Secretaría General de la entidad.

Como medidas disciplinarias, la violación de las políticas descritas, es causa de un acto administrativo y cancelación de la cuenta de acceso a los servicios de red o de correo electrónico del usuario, retiro del equipo de cómputo a su resguardo y/o hasta la destitución o de terminación contractual dependiendo de la gravedad de la violación.

Si en la revisión de los daños reportados en los equipos de cómputo sea de hardware o software se dictamina que el daño es por mal uso, descuido o negligencia, el usuario será responsable de pagar las reparaciones o la compra del bien; si el equipo es robado, perdido o dañado los gastos de la reparación, compra o deducible de la póliza de seguro.

El desconocimiento de las políticas y el uso correcto de los equipos no justifica la aplicación de las sanciones mencionadas. Es responsabilidad de cada funcionario de la entidad, usar adecuadamente los equipos asignados, según la responsabilidad de cada cargo y de acuerdo a las políticas definidas en este manual, igualmente para aquellos contratistas que por sus obligaciones deban usar equipos propios de la entidad (por ejemplo, CAD, Financiera, entre otros).

Actuaciones que conllevan a la violación de la seguridad de la información establecida por el área de TIC de Metroplús S.A.:

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
- No guardar la información digital, producto del procesamiento de la información perteneciente a la Entidad.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a la Entidad, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.

- Almacenar la información de la Entidad en los computadores personales de los usuarios.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la Entidad, para obtener, mantener o difundir material pornográfico u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma de tecnologías de la Información de la Entidad.
- Enviar sin autorización información de la Entidad a través de correos electrónicos personales.
- Enviar información pública reservada o información pública clasificada por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Usar dispositivos de almacenamiento externo en los computadores sin la autorización previa.
- Permitir el acceso de visitantes a la red corporativa, sin la autorización previa.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Entidad.
- No cumplir con las actividades designadas para la protección de los activos de información de la Entidad.
- Descuidar documentación con información crítica, reservada o clasificada de la Entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Almacenar información crítica reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a Entidad o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Entidad sin la debida autorización.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de la Entidad para beneficio personal.

- El que sin autorización acceda en todo o parte de la infraestructura informática o se mantenga dentro del mismo en contra de la voluntad de la Entidad.
- El que impida u obstaculice el funcionamiento o el acceso normal a la infraestructura informática, los datos informáticos o las redes de telecomunicaciones de la Entidad, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la Entidad.
- El que distribuya, envíe, introduzca software malicioso u otros programas de software con efectos dañinos en la plataforma tecnológica de la Entidad.
- El que modifique, altere datos personales de las bases de datos de la Entidad sin la debida autorización.
- El que superando las medidas de seguridad de la información suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Entidad.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la Entidad o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Entidad a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a la infraestructura de tecnologías de las Información de la Entidad.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por la Entidad.
- Retirar de las instalaciones de la Entidad equipos de cómputo que contengan información institucional sin la debida autorización.
- Sustraer de las instalaciones de la Entidad, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.

- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o Entidades no autorizadas.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Entidad, funcionarios o contratistas.
- Realizar cambios no autorizados en la plataforma tecnológica de la Entidad.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en los equipos de cómputo, cuyo uso no esté autorizado por el área de TIC de la Entidad.
- Copiar sin autorización las aplicaciones de software de la Entidad, o violar los derechos de autor o acuerdos de licenciamiento

| Proyectó: | Revisó: | Aprobó: |
|---|---|---|
| Mitsy Albany Mejía Medina<br>Profesional Universitario Gestión TIC y Servicios Administrativos | Víctor Julián Rivera Ocampo<br>Profesional de Calidad | Comité operativo<br>Acta 003-2022<br>30 de junio de 2022 |