# Política de seguridad de la información

## Tabla de contenido

## 1. OBJETIVO

Establecer una Política de seguridad de la información junto con los procedimientos, mecanismos, controles y herramientas adecuadas que garanticen la integridad, disponibilidad y confidencialidad de los activos de información en Metrolínea S.A.

## 2. OBJETIVOS ESPECÍFICOS

1. Minimizar el riesgo de los procesos misionales de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de los funcionarios, contratistas y terceros.
5. Apoyar la innovación tecnológica.
6. Implementar el sistema de gestión de seguridad de la información.
7. Proteger los activos de información.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
9. Fortalecer la cultura de seguridad de la información en servidores públicos, terceros, aprendices, practicantes y clientes de METROLÍNEA S.A.
10. Garantizar la continuidad del negocio frente a incidentes.

## 3. ALCANCE

La Política de Seguridad de la Información aplica para todos servidores públicos de la entidad en todos los niveles jerárquicos, a los contratistas y la ciudadanía en general.

## 4. DESCRIPCIÓN DE LA POLÍTICA

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de METROLINEA S.A. respecto a la protección de los activos de información (los servidores públicos, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Para Metrolínea S.A. la información es un activo valioso para la toma de decisiones, la gestión del cambio y el conocimiento; así como la apropiación de la política de Gobierno Digital, para establecer una política de seguridad de la información que ha de brindar a los usuarios y ciudadanos las herramientas para la defensa de lo público.

La necesidad de mitigación de riesgos alrededor de la información requiere planes de manejo de incidentes y herramientas para respaldar las actividades ejecutadas en Metrolínea S.A considerando que las TIC son un proceso de apoyo a toda la entidad. Además de incentivar la cultura de seguridad de la información a los usuarios ante ataques informáticos, virus, robos o pérdidas de información.

Es de vital importancia la gestión del conocimiento y las revisiones de la política que lleven a una mejora continua para lograr un mejor desempeño de las actividades y la articulación de la

normatividad colombiana e internacional en protección de datos, delitos informáticos y seguridad de la información además de tendencias tecnológicas que puedan ser implementadas entorno a la eficacia de las actividades relacionadas, considerando siempre los tres principios de la seguridad de la información: Confidencialidad, disponibilidad e integridad.

## 5. PROPIEDAD DE LA INFORMACIÓN

Metrolínea S.A establece la propiedad sobre los activos de información que están relacionados con su actividad. La información es entregada para su uso, operación o custodia a los servidores públicos, contratistas o terceros, de acuerdo a la función específica y necesidades del trabajo a realizar, además sin alterar en ningún momento la propiedad de los mismos. Por lo tanto, las personas responsables de los procesos que controlan activos de información o digitales, lo hacen para su manejo operativo y de conservación sin perjuicio para Metrolínea S.A. de perder la propiedad de la información.

## 6. GESTIÓN DE ACTIVOS

Los activos de información o digitales en Metrolínea S.A. se gestionarán de manera que:

1. Se encontrarán inventariados
2. Serán asignados a un responsable
3. Se realizará una valoración de riesgos.
4. Protegidos de acuerdo a su riesgo asignado.

## 7. CONTROL DE ACCESO

Es importante controlar el acceder a la información mediante sistemas internos, redes externas o internas y activos de información o digitales, esto implica establecer, mantener y actualizar las medidas a través de control de acceso soportados por una cultura de seguridad en la entidad y limitar el poder acceder de los usuarios hacia los activos de información aplicando políticas que permitan asignar los niveles requeridos de acuerdo a sus funciones, igualmente permitir identificar de manera inequívoca cada usuario y hacer seguimiento de las actividades que éste realiza.

## 8. ADMINISTRACIÓN DE REDES Y EQUIPOS

Los recursos informáticos de Metrolínea S.A, son elementos de apoyo a las labores y responsabilidades de los servidores públicos, contratistas y/o terceros, por esto, su uso está sujeto a las siguientes directrices:

- Los equipos de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el servidor público, contratista y/o tercero al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o de las obligaciones contraídas. Por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados.

- Sólo está permitido el uso de software licenciado por la entidad y/o aquel que sin requerir licencia sea expresamente autorizado por METROLINEA S.A., de la misma manera aplicará para el software que llegue a ser desarrollado dentro de la entidad.

- Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo o discos virtuales de red o discos externos de la entidad, archivos de video, música e imágenes que no sean de carácter institucional.

- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los recursos informáticos, además se debe tener organizado el puesto de trabajo para evitar incidentes con estos recursos.

- No está permitido por fallas en el suministro eléctrico a los equipos de cómputo, realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información.

- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los servidores públicos con funciones de soporte y/o el personal autorizado según contratos de mantenimiento y soporte que se puedan establecer con la entidad.

- Está prohibido utilizar almacenamiento externo no autorizado para almacenar información de la entidad, si llegaré el caso este solo debe ser autorizado por los servidores públicos con funciones de sistemas, solo para las funciones propias de la actividad de TI.

- METROLINEA S.A. realizará monitoreo sobre los dispositivos de almacenamientos externos, con el fin de prevenir o detectar fuga de información.

- La pérdida o daño de elementos o recursos informáticos, o de alguno de sus componentes, debe ser informada de inmediato a los servidores públicos con funciones de sistemas de METROLINEA S.A.

- La pérdida de información o de activos digitales debe ser informada con el detalle de la información extraviada a los servidores públicos con funciones de sistemas de METROLINEA S.A.

- El Profesional de Sistemas y/o quien haga sus veces, es la única persona autorizada para la administración del software, mismo que no debe ser copiado, suministrado a terceros o utilizado para fines personales.

- Para poder acceder a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales, estos deben estar autorizados y controlados por el Profesional de Sistemas y/o quien haga sus veces

- Cada vez que el servidor público, contratista y/o tercero no se encuentre en las instalaciones de Metrolínea S.A., los equipos de cómputo deben quedar apagados, con el fin de evitar el ingreso de personal no autorizado a estos recursos informáticos, además de contribuir al uso racional de la energía eléctrica.

- Es responsabilidad de cada servidor público, contratista y/o tercero velar por la seguridad de la información y controlar el acceso exclusivo a los recursos informáticos asignados a su nombre, para tal fin se recomienda que en cada ocasión que deba ausentarse de su puesto de trabajo el equipo de cómputo sea bloqueado para su ingreso.

- Está prohibido el uso de aplicaciones para el control remoto de equipos de cómputo e igualmente de aplicaciones para video conferencia que no estén autorizados por Metrolínea S.A., es responsabilidad de los servidores públicos, contratista y/o tercero de la entidad informar cuando se desea hacer uso de estas aplicaciones.

- Se debe evitar guardar documentos sobre el escritorio de trabajo del sistema operativo optando por un lugar seguro dentro del almacenamiento del equipo.

## 9. USO DE SOFTWARE Y SISTEMAS DE INFORMACIÓN

Todos los servidores públicos, contratistas y/o terceros de Metrolínea S.A. son responsables de la protección de la información que acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y/o uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los servidores públicos y/o contratistas no deben revelar éstas a terceros ni utilizar claves ajenas.

- Todo servidor público, contratista y/o tercero es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

- Todo servidor público, contratista y/o tercero es responsable de los registros y/o modificaciones de información que se hagan desde los activos digitales que estén asignados a su nombre, toda vez que las claves de acceso son de carácter personal e intransferible.

- En ausencia de los servidores públicos y contratistas, el acceso al equipo de cómputo le será inactivado con una solicitud elaborada por el área de Recursos Humanos al personal que tiene funciones de sistemas de METROLINEA S.A., con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad.

- Cuando un servidor público cesa en sus funciones o culmina la ejecución de su contrato laboral con Metrolínea S.A., todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente previo aviso del área de Recurso Humano; la información del servidor público será almacenada en un repositorio de la Entidad, para el

caso de los contratistas el supervisor del contrato es el encargado de informar al personal de sistemas.

- Solo las aplicaciones aprobadas por el área de sistemas de Metrolinea S.A. serán instaladas y utilizadas en cada dispositivo destinado al procesamiento de información, además de garantizar el licenciamiento para su uso.

## 10. CORREO ELECTRÓNICO

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los servidores públicos, contratistas y/o terceros de Metrolínea S.A., con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad, por lo tanto, la responsabilidad del contenido es netamente del autor.

- Está prohibido el uso de correos masivos tanto internos como externos, solo está autorizado para esto la lista institucional creada para este fin.

- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado al personal que tiene funciones de sistemas adscritos a la Secretaria General de METROLINEA S.A. No está permitido el envío y/o reenvío de mensajes en cadena.

- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado al personal que tiene funciones de sistemas adscrito a la Secretaria General de METROLINEA S.A.

- La cuenta de correo institucional no debe ser revelada en páginas o sitios ajenos a los fines de la Entidad.

- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibido distribuir información de Metrolínea S.A., no pública, a otras entidades o ciudadanos sin la debida autorización de la Gerencia.

- El Profesional de Sistemas y/o quien haga sus veces, es la única persona autorizada para la administración de la plataforma de correo electrónico.

## 11. USO DE INTERNET

Metrolínea S.A. establecerá reglas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, previa validación. Para el buen uso de los recursos de navegación de la entidad se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales.

- Los servicios a los que un determinado usuario (servidor público, contratista y/o tercero) pueda acceder desde internet dependerán del rol o funciones que desempeña el usuario en Metrolínea S.A., lo anterior será determinado por el jefe o director de cada dependencia. 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.

- Todo usuario es responsable de informar al personal que tiene funciones de sistemas los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro de Metrolinea S.A.

- Está expresamente prohibido el envío, y/o descarga, y/o visualización, de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas, y/o de procedencia desconocida que puedan causar cualquier tipo de daños en los equipos y redes.

- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.

- Metrolínea S.A. se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos sus servidores públicos o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

- El Profesional de Sistemas y/o quien haga sus veces, es la única persona autorizada para la administración de la red de datos de la entidad.

## 12. RESPONSABILIDADES Y CONTRASEÑAS

Todos los servidores públicos, contratistas y/o terceros que hagan uso de los activos de información de Metrolínea S.A., tienen la responsabilidad de seguir las reglas establecidas en la presente política y los documentos anexos a la misma, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la seguridad de información.

La gestión de usuarios se asignará con previo conocimiento de las funciones a implementar en Metrolínea S.A., por lo tanto, el manejo de documentos, cuentas de correo, accesos a sistemas de información y activos de información es responsabilidad de cada usuario, por lo cual la sensibilización de los usuarios frente a sus responsabilidades ha de ser constante.

## 13. SEGURIDAD FÍSICA

Hace referencia al tratamiento de amenazas tales como acceso no autorizado, robo, pérdida, daño, entre otros (riesgos físicos y ambientales) que puedan afectar los activos de información, medios de procesamientos y comunicaciones, así como las instalaciones donde se encuentran ubicados. Esto es el control de medios extraíbles, control sobre dispositivos a puertos de red y seguridad del entorno.

**Escritorios limpios:**

1. Cuando el servidor público y/o contratista se ausente de su lugar de trabajo, debe bloquear su estación de trabajo y debe guardar en un lugar seguro y bajo llave cualquier medio magnético removible que contenga información sensible.
2. 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.
3. 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.
4. No ingerir alimentos y bebidas en los puestos de trabajo.

**Pantallas limpias:**

1. Las estaciones de trabajo fijas y los equipos portátiles, deben tener configurado un estándar de protector de pantalla, de forma que se active ante un tiempo de como máximo cinco (05) minutos sin uso.
2. La pantalla de autenticación para el acceso a la red de la organización debe solicitar únicamente el ID de usuario y la contraseña.
3. Cuando el servidor público y/o contratista 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.

**Retirada segura de equipos:**

1. 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.
2. 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).

## 14. GESTIÓN DE RIESGOS

Metrolínea S.A. deberá realizar todas las acciones con el fin de minimizar los riesgos de la entidad establecidos en el mapa de riesgo institucional, especialmente los relacionados con la información de la organización. La gestión del riesgo tendrá en cuenta lo siguiente:

1. Identificación de vulnerabilidades y amenazas sobre los activos de información.
2. Identificación de Riesgos, Evaluación de Riesgos
3. Monitoreo
4. Planes de Acción / Tratamiento
5. Criterios de Aceptación de riesgos

## 15.GESTIÓN DEL CONOCIMIENTO

La documentación relacionada con la seguridad de la información es de vital importancia para el proceso de mejora continua y para cumplir con criterios de calidad propuestos por el sistema de gestión de calidad y seguridad de la información. Los procesos de mejora continua han de establecer las mediciones y revisiones periódicas de las políticas, manuales y procedimientos para lograr dicho objetivo.

## 16.GESTIÓN DE INCIDENTES

Metrolínea S.A. a través del personal de sistemas establecerá los procedimientos de preparación, detección y análisis, contención / respuesta, erradicación y recuperación.

## 17.CONTINUIDAD DEL NEGOCIO

Se deberá desarrollar planes de continuidad para aquellos servicios que son críticos para Metrolínea S.A. Los planes deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas, probarse y revisarse de manera periódica.

## 18.NORMATIVIDAD

La política de seguridad de la información de Metrolínea S.A. se basa en los lineamientos dados por el decreto 1008 de 2018 para la implementación de Gobierno Digital, el cual establece el habilitador Transversal de Seguridad de la información para implementación de la estrategia de Gobierno Digital, articulándose con toda la normatividad vigente en la ley colombiana en cuanto a delitos informáticos, protección de datos personales y transparencia. Además, vincula los derechos intelectuales sobre desarrollos de aplicativos y el manejo de la información dentro de la entidad basada en las recomendaciones de la ISO 27000. Habilitador Transversal de Seguridad de la información: busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información -MSPI, que contempla 6 niveles de madurez.

| CUADRO DE APROBACION | | | | |
|---|---|---|---|---|
| | **CARGOS** | **NOMBRE** | **FECHA** | **FIRMA** |
| **ELABORADO POR:** | P.U.I Ingeniero de Sistemas | José Eduardo Rueda Briceño | Diciembre de 2019 | |
| **REVISADO POR:** | Jefe Oficina Asesora Jurídica | Santiago Miguel Ortiz Acevedo | Diciembre de 2019 | |
| | PUI Calidad | Jorge E. Gualdrón Pérez (Asignado funciones Res. 209 2019) | Diciembre de 2019 | |
| **APROBADO POR:** | Comité Institucional de Gestión y Desempeño | Directores Dependencias | Diciembre de 2019 | |

| CONTROL DE CAMBIOS | | | |
|---|---|---|---|
| **VERSIÓN** | **FECHA DE REVISIÓN** | **SOLICITUD N°** | **DESCRIPCIÓN DEL CAMBIO** |
| 00 | 2018 | -- | Emisión inicial |
| 01 | 18/12/2019 | 01 | La política se ajustó a los requerimientos frente a la seguridad física de la información. |