# POLÍTICA DE SEGURIDAD Y MANEJO DE LA INFORMACIÓN

| CONTROL DE CAMBIOS | | |
|---|---|---|
| **Fecha** | **Versión** | **Descripción del cambio** |
| 22/03/2018 | 01 | Creación del documento. |
| 27/06/2019 | 02 | Se actualiza el documento en el manejo de instrumentos de gestión de la información pública. |
| 10/01/2020 | 03 | Se actualiza el documento en el control de roles y cargos en los Sistemas de Información |
| Ver firma digital de aprobación del documento | 04 | Se actualiza el documento de acuerdo con el cambio en la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 del DAFP |

| Elaboró | Revisó | Aprobó | Aprobó SIG |
|---|---|---|---|
| Juan David Vallejo Profesional grado 04 Gerencia Administrativa y Financiera | Jean Louis Torrado Gómez Profesional Especializado grado 06 Gerencia Administrativa y Financiera | Carlos Humberto Moreno Bermúdez Gerente Administrativo y Financiero | Claudia Marcela Galvis Russi Representante SIG |

Diana Marcela Aponte Peláez – Profesional Oficina Asesora de Planeación Institucional

**CONTENIDO**

## 1 INTRODUCCIÓN

El objetivo de este documento es el de documentar y otorgar lineamientos para implementar y mantener el sistema de seguridad de la información y digital de tal forma que se asegure la disponibilidad, integridad y confidencialidad. En este sentido, a través de la presente política se formaliza el compromiso con la Seguridad de la Información y se brindan los parámetros para proteger los Activos de Información de posibles amenazas.
El proceso Gestión de Seguridad de la Información se apoya en los lineamientos definidos por la estrategia de Gobierno Digital (GEL), la Política de Seguridad Digital del Modelo Integrado de Planeación y Gestión (MIPG), Ley 1712 de 2014 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas y aquellos que imparta la Alta Consejería Distrital TIC.

## 2 GENERALIDADES

El Acuerdo Distrital 642 de 2016 del Concejo de Bogotá, autorizó al Alcalde Mayor de Bogotá para la creación de la Empresa Metro de Bogotá S.A., la cual se constituyó como una sociedad por acciones del orden distrital que opera como Empresa Industrial y Comercial del Estado – EICE, realizando la planeación, estructuración, construcción, operación, explotación y mantenimiento de las líneas de metro que hacen parte del Sistema Integrado de Transporte Público de Bogotá, así como la adquisición, operación, explotación, mantenimiento y administración del material rodante. Igualmente hace parte del objeto social de la Entidad, liderar, promover, desarrollar y ejecutar proyectos urbanísticos, en especial de renovación urbana, así como la construcción y el mejoramiento del espacio público en las áreas de influencia de las líneas del metro, con criterio de sostenibilidad.

En desarrollo de las funciones misionales y de apoyo que desarrolla la Empresa Metro de Bogotá S.A., la Entidad recopila, almacena, administra y trata información, la cual es generada con ocasión del proyecto de la Primera Línea del Metro de Bogotá (PLMB) y se constituye como un activo valioso de la misma; su protección es de vital importancia para el desarrollo de cualquier actividad interna y/o externa y, en la disposición final del documento, previendo las condiciones mínimas de cuidado, custodia y adecuada utilización.

Por lo anterior, y para garantizar la seguridad y el correcto manejo de la información, la Empresa Metro de Bogotá S.A., con base en los lineamientos planteados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas y en la Ley 1712 de 2014, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información; habida cuenta que toda la información en posesión, control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la ley, es necesario establecer la Política de Seguridad y Manejo de la Información.

## 3 ALCANCE

Esta Política de Seguridad y Manejo de la Información, aplica a toda la Empresa, sus servidores públicos, contratistas y quienes tengan relación directa con la Empresa Metro de Bogotá S.A., que puedan tener acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica, canales de

comunicación, bases de datos y en general los archivos informáticos que conforman el Sitio Web, Sistemas de Información y documentos físicos de la Empresa.

## 4 DEFINICIONES

**ACTIVO:** Todo lo que tiene valor para la Empresa, el cual es necesario para realizar los procesos misionales y operativos, entre los que se puede incluir información, software, equipos de tecnología, instalaciones y el equipamiento auxiliar.

**ARCHIVO:** Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (literal j) del artículo 6 Ley 1712 de 2014).

**ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN:** Área encargada dentro de la EMB, de facilitar y colaborar, desarrollar mejoras y proponer, controlar, monitorear y establecer lineamientos técnicos aplicables, relacionados con la información e infraestructura tecnológica requerida por la Empresa para su funcionamiento y operación.

**AUTENTICACIÓN:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

**AUTORIZACIÓN:** Consentimiento previo, expreso e informado de quien tiene la responsabilidad de la información, a un tercero, para que este conozca la información, con los fines que el responsable determine.

**BASE DE DATOS:** Conjunto de información perteneciente a un mismo contexto, ordenada de modo sistemático para su posterior recuperación, análisis y/o transmisión.

**CLAVE:** Contraseña o *password* es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

**CONTROL:** Una forma para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas y que pueden ser de carácter administrativo, técnico o legal.

**CORREO ELECTRÓNICO INSTITUCIONAL:** Medio mediante el cual la Empresa Metro de Bogotá S.A., a través de la red intercambia información, entre y para los servidores públicos y contratistas autorizados para su acceso.

**CUSTODIO DE LA INFORMACIÓN:** Servidor público o contratista encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra presidir el grupo de control de Seguridad de la Información para la coordinación de esfuerzos para en las iniciativas de seguridad de la información y digital.

**DATOS ABIERTOS:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. (literal j) del artículo 6 Ley 1712 de 2014).

**DISPONIBILIDAD DE LA INFORMACIÓN:** Condición de la información que se encuentra a disposición de quienes deben y estén autorizados para acceder a ella en los momentos que así se requieran.

**DISPOSITIVO MÓVIL:** Todo dispositivo portable y utilizable durante su transporte, tales como teléfonos celulares, *smartphones*, computadores portátiles, tabletas, etc.

**DOCUMENTO EN CONSTRUCCIÓN:** No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal. (literal k) del artículo 6 Ley 1712 de 2014).

**EVENTO DE SEGURIDAD:** Situación en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información y digital o fallo de las salvaguardas, o situación desconocida que podría ser relevante para la seguridad.

**GRUPO DE CONTROL DE SEGURIDAD DE LA INFORMACIÓN:** Estará integrado por delegados de todas las áreas de la EMB y será el encargado de garantizar el apoyo a todas las disposiciones y/o requerimientos de las autoridades competentes a las iniciativas de seguridad. Este comité se desarrolla dentro del "Comité Institucional de Gestión y Desempeño de la EMB", creado bajo la resolución 026 de 2018.

**HARDWARE:** Conjunto de los componentes que integran la parte material de una computadora.

**INFORMACIÓN PÚBLICA:** Es toda información que la EMB en su calidad de tal, genere, obtenga, adquiera, o controle.

**INFORMACIÓN PÚBLICA CLASIFICADA[1]:** Es aquella información que estando en poder o custodia de la EMB en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

[1] Art. 6 literal c) Ley 1712 de 2014

De ser solicitada, no se debe entregar porque vulnera otros derechos como el derecho de las personas a la intimidad (*Habeas Data*), el derecho a la vida, salud o seguridad, los secretos comerciales, industriales y profesionales.

Esta información sólo podrá ser entregada al titular de la información, a sus apoderados o a personas autorizadas claramente para acceder a esa información en específico[2].

**INFORMACIÓN PÚBLICA RESERVADA[3]:** Es aquella información que estando en poder o custodia de la EMB en su calidad de tal, es exceptuada del acceso a la ciudadanía por daño a intereses públicos.
De ser solicitada, no debe ser entregada porque su conocimiento podría causar daño a intereses públicos. En todos los casos la reserva solo puede tener origen expresamente en la Constitución o en la ley. Estas son algunas de las temáticas sobre las cuales puede existir reserva de información, de acuerdo con la Ley 1712 de 2014: defensa y seguridad nacional, relaciones internacionales, administración efectiva de la justicia, estabilidad macroeconómica y financiera, derechos de infancia y adolescencia, salud pública[4].

**INFORMACIÓN PRIVILEGIADA**: Es aquella a la cual solo tienen acceso directo ciertas personas en razón de su profesión u oficio, la cual, por su carácter, está sujeta a reserva, ya que de conocerse podría ser utilizada con el fin de obtener provecho o beneficio para sí o para un tercero[5].

**MALWARE:** Descripción general de un programa informático que tiene efectos no deseados o maliciosos, a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. El Malware es peligroso dado que busca robar información personal que pueda ser utilizada por los atacantes para cometer delitos.

**PUBLICAR O DIVULGAR:** Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión. (literal e) del artículo 6 Ley 1712 de 2014).

**SOFTWARE:** Programas, instrucciones informáticas para ejecutar tareas en uno o varios computadores.

**TECNOLOGÍA DE LA INFORMACIÓN ó TI:** Aplicaciones, información e infraestructura requerida por la Entidad para apoyar el funcionamiento de los procesos y estrategias de la EMB.

## 5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Gerente General de la Empresa Metro de Bogotá S.A. expresa su compromiso con la gestión de los riesgos de seguridad de la información y digital de la Entidad de manera efectiva a través del establecimiento del contexto,

[2] Fuente. Cartilla ¿Qué es el derecho de acceso a la información pública y para qué me sirve? Procuraduría General de la Nación, Grupo de Transparencia y del Derecho de Acceso a la Información Pública.
[3] Literal d Art. 6 Ley 1712 de 2014. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.
[4] Fuente. Cartilla ¿Qué es el derecho de acceso a la información pública y para qué me sirve? Procuraduría General de la Nación, Grupo de Transparencia y del Derecho de Acceso a la Información Pública.
[5] Circular Externa 020 de 1997 de la Superfinanciera y Circular Externa 201 7-0 1-119907 de marzo 21 de 2017 de la SuperSociedades.

identificación, análisis, evaluación, monitoreo, revisión y seguimiento de los riesgos e implementación de acciones de control para su mitigación, con el fin de contar con un aseguramiento razonable al logro de los objetivos y metas institucionales y así mismo fomentar una cultura de riesgo a todos los niveles de la organización.

Para la Empresa Metro de Bogotá S.A. la información es vital para el desarrollo de sus actividades y es una herramienta de gran importancia para el desarrollo de su objeto y la toma de decisiones, siendo este el motivo por el cual, ésta se compromete a proteger la información, dirigiendo esfuerzos para la preservación de la confidencialidad, integridad, disponibilidad, y la creación de cultura y conciencia de seguridad en los servidores públicos, contratistas, proveedores y personas que hagan uso de la misma; siendo importante para el buen desarrollo de las labores de las personas que la utilizan, y los controles establecidos en las políticas de seguridad descritas en el presente documento, considerando que la Empresa garantizará el soporte necesario para las actividades de seguridad de la información y digital.

**Roles y responsables**

El responsable de la gestión de la seguridad de la información y de la seguridad digital es el líder de la Gerencia Administrativa y Financiera, quien se apoyará en el líder del grupo de TI, el cual tendrá a su cargo las siguientes responsabilidades:

1. Actualizar el procedimiento para la identificación y valoración de los activos de la entidad, de acuerdo a los criterios de seguridad de la información (confidencialidad, integridad y disponibilidad).
2. Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (identificación, análisis, evaluación y tratamiento).
3. Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
4. Apoyar en el seguimiento a los planes de tratamiento de riesgos definidos.
5. Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

La Entidad para lograr el objetivo necesita de la participación de los siguientes actores:

**a)** Miembros de la Junta Directiva.
**b)** El Gerente General.
**c)** Servidores públicos de la Empresa Metro de Bogotá S.A., contratistas o proveedores.
**d)** Terceros autorizados previamente para acceder a la información.

En el documento Manual para la gestión de riesgos institucionales en la EMB, codificado en el SIG como GR-MN-001, se encuentran identificadas las responsabilidades de las líneas de defensa establecidas por MIPG.

Estos, serán responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Empresa, dada su interacción con el acceso y manejo de la información que por el ejercicio del cargo administran.

**Contexto interno y externo de la Entidad**

El contexto interno y externo de la Entidad se encuentra establecido en el documento Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, identificado en el SIG con el código SI-DR-005.

### 5.1. SEGURIDAD DE LA INFORMACIÓN Y DIGITAL EN LA GESTIÓN DEL PROYECTO.

La EMB identificará y evaluará los riesgos de seguridad de la información y digital y definirá los controles de seguridad que aporten a su mitigación.

### 5.2. DISPOSITIVOS MÓVILES

Los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD, DVD, dispositivos personales USB, discos duros externos, iPod, cámaras fotográficas, cámaras de video, celulares, entre otros, estarán controlados, de acuerdo con los permisos de acceso y uso como medio de almacenamiento.

La información CLASIFICADA o RESERVADA que se desee almacenar en medios removibles debe cumplir con las disposiciones de seguridad indicadas por el Área de Tecnología de la Información, específicamente aquellas referentes al empleo de técnicas de cifrado.

El Área de Tecnología de la Información puede restringir la conexión de medios de almacenamiento removibles a los equipos de cómputo que sean propiedad de la Empresa Metro de Bogotá S.A. o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción conducente a evitar la fuga de información de la Empresa, a través de medios removibles.

Los medios de almacenamiento removibles que se conecten a los equipos de cómputo que sean propiedad de la EMB o que estén bajo su custodia, estarán sujetos a monitoreo por parte del Área de Tecnología de la Información.

El retiro de medios de almacenamiento de las instalaciones de la EMB, tales como discos duros externos que pertenezcan a la Empresa, están sujetos a la aprobación de los Gerentes o Jefes de Oficina.

Los medios de almacenamiento removibles deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante. Adicionalmente, se debe hacer seguimiento al deterioro que sufren para garantizar que la información sea transferida a otro medio, antes de que esta quede inaccesible.

En el marco de la presente política, se implementarán en La Empresa Metro de Bogotá S.A. las siguientes disposiciones, con el objetivo de proteger la información que se encuentra almacenada en dispositivos móviles y gestionar sus riesgos asociados:

**a.** Para el uso de los equipos portátiles de propiedad de la Empresa Metro de Bogotá S.A. fuera de las instalaciones, se deberá solicitar autorización ante el superior jerárquico, la cual debe estar debidamente aprobada.

**b.** Una vez autorizada la salida del equipo, el área de tecnología debe verificar que contenga controles tales como antivirus, cifrado de datos, restricción en la ejecución de aplicaciones, restricción de conexión de dispositivos USB, protección física mediante la guaya de seguridad, desactivar accesos inalámbricos cuando se encuentren conectadas a la red LAN.

**c.** Los dispositivos móviles que son propiedad de la Empresa y contengan cualquier información relevante a la operación de la misma, deben tener un sistema de autenticación.

**d.** Los dispositivos móviles que son propiedad de la Empresa y contengan cualquier información relevante a la operación de la misma, deben tener instalado un software de antivirus.

**e.** Los dispositivos móviles que son propiedad de la Empresa y contengan cualquier información relevante a la operación de la misma, deben tener un control sobre el tipo y la versión de aplicaciones instaladas, al igual que deben estar sometidos a restricciones de conexión hacia ciertos servicios de información que sean considerados malware.

Los anteriores literales, serán controlados y monitoreados por el área TI de la EMB.

### 5.3. USO DE INTERNET

Quien pretenda el acceso al servicio, deberá tener algún tipo de vinculación con la Empresa Metro de Bogotá S.A.; si es servidor público deberá diligenciar solicitud de acceso a servicios tecnológicos, que el Área de Tecnologías de la Información suministrará.

Este servicio debe utilizarse única y exclusivamente para las tareas propias de la función o actividad desarrollada en la EMB, y no debe utilizarse para ningún otro fin.

No se permite la conexión de módems externos o internos, que no estén autorizados por el Área de Tecnologías de la Información.

No se permitirá el acceso a páginas relacionadas con actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, pornografía,

*spyware*, *adware*, redes *peer to peer* (P2P), o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos del Área de Tecnologías de la Información.

El Área de Tecnologías de la Información velará por no permitir la instalación, descarga, intercambio y/o uso, de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, que de alguna forma atenten contra la propiedad intelectual, o que contengan archivos ejecutables, herramientas de *hacking*, entre otros.

Cada uno de los servidores públicos y contratistas será responsable de dar un uso adecuado de este recurso y en ningún momento podrá utilizar este, en prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información y digital, entre otros.

El uso del servicio de internet podrá ser utilizado para uso personal de los servidores públicos, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la Empresa.

### 5.4. USO REDES SOCIALES

Los autorizados para usar los servicios de redes sociales son responsables de la información, para evitar prácticas que puedan poner en riesgo la seguridad de la información y digital que tienen a su cargo; de igual forma todas las comunicaciones establecidas mediante este servicio pueden ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

La Empresa a través del área de TI, al facilitar el acceso al uso de redes sociales y teniendo en cuenta que constituyen un complemento a muchas actividades que se realizan por estos medios, verificará que quienes la utilicen lo hagan de forma correcta y moderada y debe ser utilizado para actividades relacionadas con el ejercicio de sus actividades, funciones u obligaciones ya que todas las comunicaciones establecidas mediante este servicio podrán ser monitoreadas por el administrador del servicio.

Solo quienes estén autorizados en razón a sus funciones o por designación realizada de manera clara, expresa y escrita, podrán crear cuentas, abrir grupos, y publicar información escrita o audiovisual a nombre de la Empresa Metro de Bogotá S.A.

El Área de Tecnología de la Información es responsable de administrar las plataformas tecnológicas que soportan el acceso a la red/cuentas de usuario y/o al servicio de Internet para los servidores públicos que desempeñen labores en la EMB.

El Área de Tecnología de la Información se reserva el derecho de monitorear las comunicaciones y/o información que presenten un comportamiento inusual o sospechoso.

Según la disponibilidad de los recursos de transmisión y acceso a internet con los que cuente la EMB, se autorizará el uso y limitaciones en el acceso a las plataformas de redes sociales.

El Área de Tecnología de la Información será la encargada de determinar las directrices y lineamientos para el uso de los diferentes sistemas o plataformas de redes sociales en la Empresa, según las necesidades.

El uso y la finalidad de las redes sociales de la EMB, se debe limitar a la divulgación de las actividades directas o indirectas que desarrolla la Empresa. Resulta importante informar que la Empresa dispone de diferentes medios idóneos para presentar las PQRS, de los cuales se excluyen las redes sociales.

## 5.5. SEGURIDAD DE LA INFORMACIÓN EN RECURSOS HUMANOS

### 5.5.1. SELECCIÓN DE PERSONAL Y CONTRATACIÓN

En el proceso de selección de personal de planta o contratistas, se deben incorporar mecanismos para establecer la idoneidad del candidato para el manejo de la información a la cual deba acceder en ejercicio de su cargo u obligación. El proceso debe ser documentado por el responsable y las evidencias deben hacer parte del expediente físico.

### 5.5.2. DESVINCULACIÓN DE PERSONAL

Cada servidor y contratista tiene un deber de reserva de información después de su desvinculación de la Empresa hasta por el término de dos (2) años. El incumplimiento de las normas de reserva es causal de falta disciplinaria y puede dar lugar, adicionalmente, a la comisión de hechos punibles consagrados en el Código Penal Colombiano.

### 5.5.3. ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

El acuerdo de confidencialidad y no divulgación, contiene un compromiso por medio del cual todo servidor, contratista y/o tercero vinculado a la Entidad, deberá firmar su compromiso de no divulgar la información interna y externa que conozca de la Empresa, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo servidor, contratista y/o tercero, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

Los servidores públicos deben firmar la cláusula y/o acuerdos de confidencialidad definidos por la EMB y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Empresa a personas o entidades externas. Su aplicación se llevará a cabo en coordinación con la Gerencia de la EMB, que por algún motivo deba firmar acuerdos

de confidencialidad con terceros o contratistas, que por diferentes razones requieran conocer o intercambiar información restringida o confidencial. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

El acuerdo de confidencialidad deberá formalizarse en cada uno de los contratos celebrados con terceros y que en la prestación del servicio puedan tener acceso a la información reservada o confidencial. De dicho acuerdo deberá derivarse una responsabilidad, tanto civil como penal, para la tercera parte que la Empresa Metro de Bogotá S.A. contrata; esto de conformidad con las leyes de protección de datos aplicables.

Todos los servidores públicos y contratistas de la EMB deben guardar absoluta reserva en relación con la información a la que tengan acceso con ocasión de la ejecución del contrato, aun después de finalizada su ejecución, por el tiempo establecido por la normatividad legal vigente y aplicable para cada caso en particular.

## 5.6. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y DIGITAL

Las etapas de gestión y administración de los riesgos de seguridad de la información y digital se encuentran consignadas en el documento SI-DR-005, Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información.

## 5.7. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE ACTIVOS DE INFORMACIÓN

### 5.7.1. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La identificación y clasificación de los Activos de Información se realizará de acuerdo con la criticidad, sensibilidad y reserva de ésta, siguiendo los criterios de Confidencialidad, Integridad y Disponibilidad de la información y los lineamientos para la divulgación de la información pública considerados en el Índice de Información Clasificada y Reservada y en las Tablas de Control de Accesos, instrumentos definidos dentro del Proceso de Gestión Documental, siguiendo los parámetros establecidos en el modelo nacional de Gestión de Riesgos de Seguridad de la Información, anexo a la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

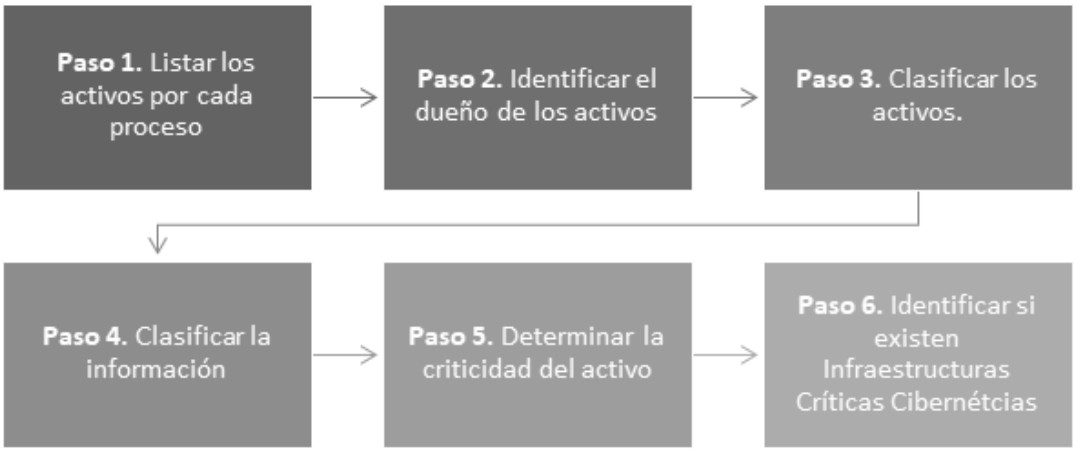


*Ilustración 1. Pasos para la identificación y valoración de activos – Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Departamento Administrativo de Función Pública*

La actualización del Registro de Activos de Información que soportan los procesos de negocio será responsabilidad del líder de cada proceso, el cual debe estar en capacidad de clasificarlo y definir el nivel adecuado de protección que requiera. La periodicidad de la actualización del registro mencionado debe estar definido en el proceso de Gestión Documental del Sistema Integrado de Gestión de la Empresa.

### 5.7.2. ETIQUETADO DE LA INFORMACIÓN

Toda la información debe ser etiquetada por cada servidor y contratista de acuerdo con la clasificación del tipo de activo de información a que pertenece, según la identificación de activos realizada por la Empresa y que está definido en el Índice de Información Clasificada y Reservada dentro del proceso de Gestión Documental.

### 5.7.3. GESTIÓN DE RECURSOS TECNOLÓGICOS

La Empresa, a través de la Gerencia Administrativa y Financiera, gestiona y pone a disposición de los servidores públicos y contratistas recursos tecnológicos, los cuales deben custodiar, cuidar y dar buen uso.

La Empresa se reserva el derecho de monitorear el acceso y uso de los recursos tecnológicos asignados a los servidores o contratistas. La Gerencia Administrativa y Financiera es la dependencia encargada de hacer las modificaciones o actualizaciones en los elementos y recursos tecnológicos.

#### 5.7.4. ACCESO A LA RED INTERNA

La Empresa, a través del área de TI, debe autorizar el acceso a la red interna o intranet de los dispositivos personales de servidores, contratistas y terceros, tales como teléfonos celulares, tabletas o portátiles.

La Empresa, restringe el uso de la red interna para difundir material relacionado con pornografía, información personal o cualquier otro contenido que vaya en contra del código de integridad de la Empresa.

### 5.8. SEGURIDAD PARA EL CONTROL DE ACCESO LÓGICO

#### 5.8.1. CONTROL DE ACCESO CON USUARIO Y CONTRASEÑA

El acceso a las plataformas tecnológicas y sistemas de información que disponga la Empresa se debe realizar a través de un usuario y contraseña que garanticen la confidencialidad y su uso es personal e intransferible.

**A.** La clave establecida por cada usuario debe cumplir con lo siguiente:

Tener mínimo ocho (8) caracteres alfanuméricos.

La contraseña debe cumplir con tres de los cuatro requisitos a saber:
- Caracteres en mayúsculas.
- Caracteres en minúsculas.
- Base de 10 dígitos (0 a 9).
- Caracteres no alfabéticos (Ejemplo:., ¡,$,%,&).

**B.** Cada vez que se cambie la contraseña, esta debe ser distinta por lo menos de las últimas cinco anteriores, conservando historial de contraseñas.
**C.** El usuario puede cambiar su contraseña de forma voluntaria cada vez que lo requiera
**D.** Después de tres (3) intentos de acceso fallidos consecutivos se debe bloquear el usuario y solo se puede desbloquear a través del usuario Administrador
**E.** La sesión del usuario se debe bloquear después de cinco (5) minutos de inactividad
**F.** Las Contraseñas se deben almacenar de forma cifrada
**G.** El usuario Administrador no debe tener acceso a la visualización de claves de los usuarios. Se exceptúan aquellas plataformas tecnológicas que la Empresa considere de acceso público y que por ende no requieren autenticación.
**H.** La Empresa mantendrá los mecanismos de control de acceso con usuario y contraseña para asegurar que los activos de información estén siempre protegidos.

Corresponde a cada servidor dar el debido manejo a los usuarios y contraseñas que en el ejercicio de sus funciones le sean asignadas. Cualquier irregularidad en el manejo de estas, deberá ser asumida de manera inicial por el servidor público a quien estén asignadas.

Corresponde al área de TI de la EMB, garantizar semestralmente los estándares de seguridad de la información y digital y establecer controles que puedan ser reportados a la Gerencia Administrativa y Financiera.

### 5.8.2. CONTROL DE ROLES VS CARGOS A LOS SISTEMAS DE INFORMACIÓN

Para el control de accesos a los Sistemas de Información, la Entidad deberá realizar la certificación de usuarios de forma anual teniendo en cuenta los siguientes lineamientos:

- Realizar anualmente la inactivación de los usuarios de los sistemas de información vigentes
- Realizar un análisis de los perfiles y roles actuales de los sistemas de información según los distintos cargos desempeñados en la Empresa; lo anterior deberá dejar como entregable un matriz de roles vs cargos, para cada uno de estos sistemas. Los nuevos perfiles y roles por cargos en cada sistema definidos en el entregable (matriz de roles vs cargo) deberán ser revisados y aprobados por las áreas funcionales (Dueño de los datos), y responsables de velar por la seguridad de la información y digital y la gestión de riesgos al interior de la Empresa.
- Validar la relevancia de mantener los roles y responsabilidades asignados a cada usuario con los jefes y/o Gerentes responsables del servidor público o contratista dueño de la cuenta
- Las diferencias identificadas serán reportadas al área de tecnología para que se realicen los correctivos que sean necesarios en los distintos sistemas de información
- Todos los cambios que surjan del reporte de monitoreo en cada uno de los sistemas de información deberán ser realizados a más tardar a los cinco (5) días hábiles posteriores a la generación del reporte.

## 5.9. CONTROL DE ACCESO A RED DE INTERNET INALÁMBRICA

El Área de Tecnología de la Información se encargará de cambiar la clave para el acceso a la red inalámbrica METRO_INVITADOS con una periodicidad mensual.

La red inalámbrica METRO_BOGOTA será actualizada cuando haya lugar y sin previo aviso. La misma será suministrada únicamente a los servidores públicos y contratistas que utilicen computador portátil.

Corresponde a cada servidor dar un manejo diligente a las claves que le sean informadas, esto es, no informarla a terceros ni emplearla para conexiones privadas.

### 5.10. SEGURIDAD DE ESCRITORIO

Todos los servidores y contratistas de la Empresa son responsables de bloquear la sesión de su equipo de cómputo al dejar su puesto de trabajo. De igual manera, los equipos de cómputo deben tener configurado el bloqueo automático de la pantalla luego de 5 minutos de inactividad y se desbloqueará utilizando las credenciales de acceso. Si el equipo no cuenta con dicha configuración, está en la obligación de informar al Área de Tecnología de la Información.

En el caso que un servidor o contratista tenga documentos físicos o electrónicos almacenados en medios ópticos y magnéticos tipificados como información clasificada o reservada, deberá estar bajo llave cuando no se encuentre en su puesto de trabajo. Adicional a lo anterior, esta información electrónica no será compartida en carpetas de red, para evitar fuga o pérdida de la misma.

### 5.11. INSTALACIÓN DE APLICATIVOS O HERRAMIENTAS

Está completamente prohibido la instalación de aplicativos o herramientas no validadas por el Área de Tecnología de la Información, aun cuando estas sean de libre distribución o demos comerciales. Por lo tanto, de requerirse el uso de un tipo de aplicación de esta categoría, se solicitará de manera previa al Área de Tecnología de la Información su concepto, de tal manera que no se ponga en riesgo técnico, legal o de otro tipo a la Empresa.

El Área de Tecnología de la Información implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales; así mismo controlará el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.

### 5.12. SEGURIDAD EN IMPRESORAS

Los servidores y contratistas de la Empresa no deben dejar impresiones con información sensible en la bandeja de salida de las impresoras. De igual forma está prohibido utilizar la impresora para temas personales.

En materia de impresiones se privilegiará el tema de protección ambiental y austeridad, para lo cual se definirán e impartirán las instrucciones que en ese sentido se estimen pertinentes a través de la Subgerencia de Gestión Ambiental y SISO.

### 5.13. INTEGRIDAD DE LA INFORMACIÓN

Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integral, coherente y exclusivamente a las personas y a través de los medios correspondientes sin sufrir modificaciones o alteraciones, salvo que así lo determinen las personas autorizadas.

### 5.14. RESPALDO DE INFORMACIÓN PERSONAL

La información de cada servidor y contratista debe ser almacenada en los repositorios en la nube que han sido dispuestos para tal fin. El repositorio cuenta con una política de copias de seguridad que asegura el acceso o la restauración oportuna de la información en caso de ser necesario.

Es responsabilidad de cada servidor o contratista de la organización, almacenar la información en sus respectivos repositorios.

El área de Tecnologías de la Información apoyará a los servidores y contratistas que requieran asistencia en la generación de la respectiva copia de seguridad y respaldo.

### 5.15. RESPALDO DE INFORMACIÓN DE INFRAESTRUCTURA

La Empresa cuenta con una única política de *backup* la cual es incremental diario, *full* semanal con una retención de 30 días y con posibilidad de mínimo 1 restauración mensual para los servicios de infraestructura como servicio.

### 5.16. GESTIÓN DE CAMBIOS

La Empresa definió los procedimientos "IT-PR-002 Procedimiento Gestión Cambios Sistemas de Información" y "IT-PR-003 Procedimiento Gestión Cambios Infraestructura Tecnológica" dentro del Sistema Integrado de Gestión, para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

### 5.17. REGISTRO, REPORTE Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los servidores, contratistas y terceros deben estar atentos a los riesgos, vulnerabilidades o condiciones anormales que puedan afectar la Integridad, Confidencialidad y Disponibilidad de los Activos de Información de la Empresa. Así mismo, deben reportar los incidentes de seguridad que identifiquen, a través de la herramienta de gestión de TI.

La Gerencia Administrativa y Financiera, a través de los procesos de Gestión de Seguridad de la Información y Administración de Recursos de TI, realizará la evaluación de los registros y reportes consignados en los canales y procederá con la solución y reporte a los proveedores que haya lugar.

### 5.18. REPORTE DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El responsable de la seguridad de la información deberá reportar una vez al año a la alta dirección en el comité institucional de gestión y desempeño y al comité institucional de coordinación de control interno, la información correspondiente a la gestión de riesgos de seguridad digital, o cuando ocurra un cambio

en la estructura organizacional o en el mapa de procesos de la entidad que genere un impacto en las operaciones o afecte los riesgos identificados.

### 5.19. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La Empresa mantendrá un programa de capacitación y sensibilización en Seguridad de la Información que busque el crecimiento continuo de la conciencia individual y colectiva para la protección de los Activos de Información.

De igual forma, el Área de Tecnología de la Información comparte y aplica las recomendaciones recibidas por las entidades que realizan el acompañamiento en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado por la Empresa.

Es obligación de los servidores y contratistas de la Empresa asistir a las capacitaciones y charlas programadas sobre Seguridad de la Información.

### 5.20. SEGURIDAD DE LAS COMUNICACIONES

#### 5.20.1. USO DE CORREO ELECTRÓNICO CORPORATIVO

Las cuentas de correo electrónico de los servidores públicos y contratistas de la Empresa son corporativas y de uso exclusivo para el desarrollo de sus actividades, funciones u obligaciones. Por lo tanto, la información gestionada a través de este medio es propiedad de la EMB y cada usuario como responsable de su buzón debe cumplir con las condiciones de seguridad definidas.

Los servidores y contratistas no deben utilizar el correo electrónico para el envío de cadenas de correo, mensajes con contenido religioso, político, racista, pornográfico o cualquier tipo de mensaje que atente contra la integridad de las personas, las leyes y la moral. Adicionalmente, el correo electrónico no debe ser utilizado para actividades que comprometan el buen nombre, los Activos de Información o los recursos de la Empresa.

#### 5.20.2. ADQUISICIÓN Y MANTENIMIENTO DE TECNOLOGÍA

La Gerencia Administrativa y Financiera es la encargada de definir las aplicaciones y periféricos a adquirir, de acuerdo con los requerimientos de las demás áreas. De esta manera se garantiza la conveniencia, soporte, mantenimiento y seguridad de la infraestructura tecnológica, software y sistemas de información.

### 5.20.3. ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN

La construcción y modificación de sistemas de información o la implementación de nuevos módulos a los sistemas de información misionales o de apoyo, desarrollados al interior de la Empresa o contratados con terceras partes, deben estar acordes con el documento "IT-DR-003 Directriz para Contratación de Sistemas de Información".

### 5.20.4. CUMPLIMIENTO DE REQUISITOS LEGALES DE SOFTWARE

La Empresa acata las normas legales existentes relacionadas con seguridad de la información y digital, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables y relacionados con la protección de derechos de autor y propiedad intelectual, por lo que a través del Área de Tecnología de la Información se revisará que los software instalados en los equipos de los servidores públicos cumpla con los requerimientos legales y de licenciamiento aplicables.

El Área de Tecnología de la Información deberá garantizar que todo el software que ejecute los activos de información de la Empresa esté protegido por derechos de autor y requiera licencia de uso o, sea software de libre distribución y uso.

Los servidores de la Empresa deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software; se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y la reproducción no autorizada es una violación a la ley.

## 6 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Para el adecuado tratamiento y protección de la información, la Empresa Metro de Bogotá S.A. debe realizar una clasificación.

### 6.1. CLASIFICACIÓN DE LA INFORMACIÓN

La información que pertenezca a la EMB estará identificada en el Registro de Activos de Información[6], el cual relaciona de forma organizada toda la información que se encuentra en posesión, custodia o bajo control de la Entidad, independiente de su soporte. El Registro de Activos de Información recoge las series, subseries y tipologías documentales definidas en las Tablas de Retención Documental, la información y documentos publicados en el sitio web de la Empresa y demás información disponible en distintos medios o soportes, por ejemplo, las bases de datos.

[6] Véase Ley 1712 de 2014, art. 13, Decreto 105 de 2015, art, 37 y 38.

Por otro lado, la Tabla de Control de Acceso[7], tomando como insumo el Registro de Activos de Información, tipificará la información en Pública, Clasificada y Reservada; así mismo, indicará allí las personas naturales y/o jurídicas que pueden acceder a las diferentes categorías de información.

De igual manera, el Índice de Información Clasificada y Reservada[8], traerá de las Tablas de Control de Acceso, la información definida como Clasificada y Reservada, especificando, entre otros campos, el objeto legítimo de la excepción, el fundamento constitucional y legal, el fundamento jurídico de la excepción y precisando si la excepción sobre la información es total o parcial. Este Índice cumplirá esencialmente dos funciones: por un lado, sirve a los servidores y contratistas y ciudadanos para conocer cuáles categorías de información tienen acceso restringido y, por otro, servir de herramienta para ofrecer respuesta a las solicitudes asociadas al acceso a la información clasificada y reservada, conforme a lo definido en el Decreto 1080 de 2015, art. 2.8.4.4.1.

La Gerencia Administrativa y Financiera, en conjunto con las dependencias de la Empresa Metro de Bogotá, son los responsables de definir las pautas para la identificación y las medidas de tratamiento o de manejo de la información conforme con los procesos y su valor legal, administrativo, técnico, científico y cultural.

Por último, se encuentra el Esquema de Publicación[9] , instrumento que se debe disponer para dar cuenta de la información publicada en el sitio web de la Empresa www.metrodebogota.gov.co y que, en ciertos casos, se encuentra disponible en otros soportes; este Esquema debe contener la información mínima exigida en la Ley 1712 de 2014, artículos 9, 10 y 11, la Ley 1474 de 2011 y demás normas vigentes.

### 6.2. ETIQUETADO Y MANEJO DE INFORMACIÓN

Cada servidor público y contratista de la Empresa Metro de Bogotá S.A. deberá mantener organizado el archivo de gestión, acatando las orientaciones y los lineamientos establecidos por la Gerencia Administrativa y Financiera.

Los servidores y contratistas de la Empresa Metro de Bogotá S.A. son responsables de la producción, gestión y trámite, organización y conservación de los documentos.

Las Gerencias y Oficinas Asesoras de la EMB deben conservar y custodiar en el área de archivo determinada, la documentación en forma organizada, de acuerdo con los tiempos de retención estimados en la Tabla de Retención Documental de la Empresa, los procedimientos, instructivos, entre otros. Las áreas de archivo serán de acceso restringido y solo ingresará el personal que esté autorizado por el líder del proceso o área.

[7] Véase Decreto 1080 de 2015, art. 2.8.2.5.8, literal i.
[8] Véase Ley 1712 de 2014, art. 20, Decreto 103 de 2015, art. 39 y 40.
[9] Véase Ley 1712 de 2014, art. 12, Decreto 103 de 2015, art. 41 y 42.

El Área de Gestión Documental coordinará las transferencias documentales al archivo central y archivo histórico, de acuerdo con las Tablas de Retención Documental y el calendario anual de transferencias documentales.

Los archivos de gestión de las Gerencias y Oficinas Asesoras de la Empresa deberán relacionar sus expedientes en el formato "GD-FR-015 Formato Único Inventario Documental EMB", de acuerdo con lo especificado en la correspondiente Tabla de Retención Documental.

Los documentos en papel, electrónicos y digitales tendrán igual tratamiento conforme con los principios archivísticos y el ciclo vital de los documentos. Por lo anterior, las Tablas de Retención Documental, entre otros instrumentos archivísticos, aplicarán para todos los documentos producidos, independiente de su soporte.

La tecnología utilizada para salvaguardar, facilitar y conservar la información de los documentos en soportes informáticos debe garantizar la seguridad de no permitir alteraciones o consultas de personas no autorizadas.

### 6.3. FIRMAS DIGITALES

El área de Tecnología de la Información debe proveer los respectivos mecanismos de seguridad consignados para el tratamiento de mensajes electrónicos en la Ley 527 de 1999 y Decreto 1747 de 2000. Por lo anterior, la Empresa asignará las firmas digitales requeridas por la operación, las cuales serán instaladas por el área de Tecnología de la Información a los servidores autorizados para tal fin; cada firma es personal e intransferible, por lo que el servidor público debe hacer uso responsable de la misma.

## 7 POLÍTICA DE LA SEGURIDAD FÍSICA

Implementar el programa de seguridad física para el acceso a las instalaciones que permita fortalecer la confidencialidad, disponibilidad e integridad de la información.

El Área de Tecnología e Información debe implementar alarmas de detección de intrusos en los centros de datos y centros de cableado.

La Gerencia Administrativa y Financiera debe mantener actualizado el programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las instalaciones pertenecientes a la Empresa.

### 7.1. SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO

Además de la protección de la información en las redes, se deberá también realizar la protección de la infraestructura que la soporta.

Por lo que en el lugar donde se encuentre el centro de datos o de cableado, no está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center.
- Portar armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.

## 8 ESTÁNDARES EN EL MANEJO DE LA INFORMACIÓN

Los servidores públicos y contratistas vinculados con la Empresa, cualquiera sea la modalidad y calidad de la relación, deberán guardar cuidado especial con el manejo de la información, sobre todo en aquellos asuntos que tengan relación con la información en proceso de preparación, destinada a procesos de selección no abiertos, pendiente de aprobación y en general, toda aquella que requiera un proceso de validación, aprobación y adopción previo, para ser divulgada y publicada.

Los servidores públicos y contratistas vinculados con la Empresa, cualquiera sea la modalidad y calidad de la relación, y los contratistas de la Empresa, están obligados a utilizar la información a la cual tengan acceso en virtud de sus funciones, o relación contractual, exclusivamente para el ejercicio de las mismas, con plena observancia del procedimiento establecido para la revelación de información a terceros.

Dentro de los estándares de manejo de la información, se encuentran los siguientes:

1. **Se prohíbe el uso no autorizado de la Información**, para lo cual los servidores y contratistas de la EMB, tratarán la información con el mismo cuidado que generalmente acostumbran para proteger la información de su propiedad.

2. **El principio general** es que toda información asociada a recursos públicos es pública; sin embargo, hay cierta información cuyo acceso puede ser denegado, pues el contenido de dicha información, de ser conocido públicamente, puede afectar derechos de personas naturales o jurídicas o puede causar daño a intereses públicos. De allí surgen las categorías de información pública clasificada e información pública reservada.

3. **Documentos en construcción[10]:** Es aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal y no es considerada como información pública.

4. Para el manejo de la información deberá tenerse en cuenta **la fuente de la información**, **el uso y finalidad** de la misma:

[10] Literal k Art. 6 de la ley 1712 de 2014.

a) La fuente de la información puede ser interna (elaboración propia de la EMB) o externa (producto de los consultores, asesores, contratistas, entidades públicas o privadas asociadas al proyecto de la PLMB o a la Empresa Metro de Bogotá).

b) El uso o finalidad de la información deberá ser para:

i. El desarrollo del objeto social de la Empresa Metro de Bogotá;

ii. El desarrollo de las funciones de la Empresa Metro de Bogotá;

iii. El desarrollo de las funciones a cargo de los servidores públicos de la Empresa Metro de Bogotá (empleados públicos y trabajadores oficiales);

iv. El desarrollo de las obligaciones de los contratistas, asesores y consultores de la Empresa Metro de Bogotá;

v. El desarrollo de las funciones a cargo de los servidores públicos de las entidades públicas del orden Nacional o Distrital que deban conocer la información del proyecto de la PLMB o de la Empresa con ocasión de su cargo y sus responsabilidades;

vi. El desarrollo de las obligaciones de contratistas, asesores y consultores de las entidades públicas del orden Nacional o Distrital que deban conocer la información del proyecto de la PLMB o de la Empresa con ocasión de contrato y sus responsabilidades;

vii. El desarrollo de las funciones a cargo de los organismos de control del orden distrital y nacional.

La Empresa Metro de Bogotá S.A., definirá el protocolo de manejo de la información respecto de servidores públicos y contratistas.

## 9 CUMPLIMIENTO DE LA LEY DE TRANSPARENCIA Y DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA NACIONAL

1. La EMB cumplirá con la totalidad y postulados de la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, de conformidad con la Ley 1712 de 2014, sin que se limite a ciertos literales o numerales de la misma.

2. La EMB tendrá un sitio web que cumpla con todos los lineamientos definidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones, y publicará trimestralmente la siguiente información, adicional a la requerida por la Ley 1712 de 2014:

a. Los estados financieros y las inversiones;

b. Pagos por concepto de viáticos y gastos de desplazamiento de sus servidores, contratistas y Miembros de Junta Directiva para ejecutar sus obligaciones.

c. Información relacionada con la política de Gobierno Corporativo, asignación de citas, reportes de peticiones, quejas y reclamos, entre otros, incluyendo los requerimientos adicionales que en materia de publicidad de información determine y genere la EMB.

3. Adicionalmente, la EMB implementará un sistema de gestión documental que facilite la identificación, gestión, clasificación, organización, conservación y disposición de la información pública, desde su creación hasta su disposición final, con fines de conservación permanente o eliminación, aportando así al cumplimiento de la Ley 1712 de 2014 y el Decreto 103 de 2015.