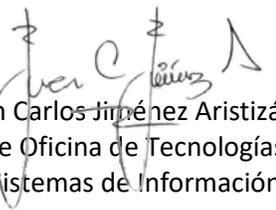


	PROCESO: GESTIÓN TECNOLÓGICA		
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS		
Fecha	Versión	Descripción del cambio
Ver firma digital de aprobación del documento.	01	En el marco de la reestructuración de la EMB, se realiza la modificación de la denominación de los procesos (De SI-Gestión de Seguridad de la Información a GT-Gestión Tecnológica) y código de documento (De SI-DR-003_V.01 a GT-DR-002_V.01), se realiza modificación general al documento.

Elaboró	Revisó / Aprobó	Aprobó SIG
 Yuly Rojas Idarraga Profesional Oficina de Tecnologías y Sistemas de Información	 Juan Carlos Jiménez Aristizábal Jefe Oficina de Tecnologías y Sistemas de Información	Claudia Marcela Galvis Russi Representante de la Alta Dirección SIG

 Diana Marcela Aponte Peláez – Oficina Asesora de Planeación

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.

 METRO BOGOTÁ	PROCESO: GESTIÓN TECNOLÓGICA		 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>REGULACIÓN Metro de Bogotá S.A.</small>
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

CONTENIDO

1.	INTRODUCCIÓN	3
2.	OBJETIVO	3
3.	ALCANCE	3
4.	NORMATIVIDAD O DOCUMENTOS.....	3
5.	DEFINICIONES, SÍMBOLOS Y ABREVIATURAS	5
6.	RESPONSABLES.....	6
7.	ACTIVIDADES Y ENTREGABLES	7

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.

	PROCESO: GESTIÓN TECNOLÓGICA		 ALCALDÍA MAYOR DE BOGOTÁ D.C. REGULACIÓN Metro de Bogotá S.A.
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

1. INTRODUCCIÓN

Este documento expone las prioridades de implementación de los controles en relación a seguridad de la información, enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar), de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI)¹ elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y de obligatorio cumplimiento por parte de las entidades del Estado; este modelo se encuentra alineado con el Marco de Referencia de Arquitectura TI², cuyo objetivo es orientar la creación o fortalecimiento de las capacidades de Arquitectura Empresarial, Gestión de Proyectos de TI, Gestión y Gobierno de TI, requeridas en los procesos de transformación digital de las entidades del Estado para lograr implementar la Política de Gobierno Digital.

Es por esto que el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios, define la seguridad de la información como principio de la Política de Gobierno Digital, así como el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

2. OBJETIVO

Presentar la implementación de controles de seguridad alineados con la política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información – MSPI y el Modelo Integrado de Planeación y Gestión – MIPG, para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información de la Empresa Metro de Bogotá S.A.

3. ALCANCE

El documento contempla desde la implementación de las actividades necesarias para lograr progresivamente el fortalecimiento del modelo del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital y conforme a la disponibilidad de los recursos con los que cuenta la Empresa Metro de Bogotá S.A. para el desarrollo y la implementación de este modelo.

4. NORMATIVIDAD O DOCUMENTOS

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De

¹ <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

² <https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8118.html>

	PROCESO: GESTIÓN TECNOLÓGICA		 ALCALDÍA MAYOR DE BOGOTÁ D.C. REGULONE Metro de Bogotá S.A.
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

LEY 23 DE 1982: Sobre Derechos de Autor.

LEY 527 DE 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 1266 DE 2008: por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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

LEY 1474 DE 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

LEY ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

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.

LEY 1915 DE 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos

DECRETO 4632 DE 2011: Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011, en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

DECRETO 2609 DE 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

DECRETO 2693 DE 2012: Estrategia de Gobierno en Línea.

DECRETO 1377 DE 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.

	PROCESO: GESTIÓN TECNOLÓGICA		 ALCALDÍA MAYOR DE BOGOTÁ D.C. REGULACIÓN Metro de Bogotá S.A.
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

DECRETO 1008 DEL 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.

DECRETO 612 DE 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11: Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

5. DEFINICIONES, SÍMBOLOS Y ABREVIATURAS

ACTIVO DE INFORMACIÓN: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

CERTIFICADO DE SITIO SEGURO (SSL): sirven para brindar seguridad al visitante de algún portal web, lo que refleja que el sitio es auténtico, real y confiable para ingresar datos. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que los datos viajen de manera íntegra y segura, por lo que son totalmente cifrados o encriptados.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

DDoS: En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (por sus siglas en inglés, Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

DIRECTORIO ACTIVO: es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable, cuando lo requiera una entidad autorizada.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

PROCESO: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.

	PROCESO: GESTIÓN TECNOLÓGICA		
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

VULNERABILIDAD: Es aquella debilidad de un activo o grupo de activos de información.

6. RESPONSABLES

Para seguir con la implementación, operación y mejora del SGSI, la Empresa Metro de Bogotá S.A. adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) y actualiza la política de seguridad y manejo de la información, asegurándose el despliegue de las directrices de seguridad en todas las dependencias de la Empresa y monitoreando constantemente su cumplimiento para tomar las acciones necesarias que permitan garantizar la seguridad de la información.

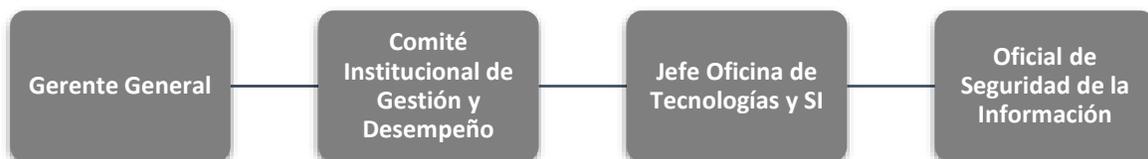
Comité Institucional de Gestión y Desempeño

La política de seguridad digital que contribuye con el desarrollo de las dimensiones de MIPG fue adoptada en la Resolución 026 de 2018 *“Por la cual se adopta el Modelo Integrado de Planeación y Gestión MIPG, se conforma el Comité Institucional de Gestión y Desempeño en la Empresa METRO de BOGOTÁ S.A., se definen sus roles y responsabilidades en la implementación, sostenibilidad y mejora del MIPG y se reglamenta el Sistema de Control Interno”*. De acuerdo con lo anterior, es responsabilidad de la Oficina de Tecnologías y Sistemas de Información suministrar y elaborar los planes, programas, proyectos metodologías y estrategias en materia de Seguridad de la Información para ser presentados en el Comité Institucional de Gestión y Desempeño.

Jefe de la Oficina de Tecnologías y Sistemas de Información

El Jefe de la Oficina de Tecnologías y Sistemas de Información asignó la responsabilidad correspondiente al rol de “Oficial de Seguridad de la Información” a través del manual de actividades al Profesional grado 03 de la OTSI, para efectos de garantizar y liderar la implementación, mantenimiento y mejora del SGSI.

El Oficial de Seguridad de la información actúa bajo las directrices que establezca el Comité Institucional de Gestión y Desempeño, el Gerente General y el Jefe de la Oficina de Tecnologías y Sistemas de Información así:



En consecuencia, el Oficial de Seguridad de la información, planea, diseña e implementa el SGSI de la Empresa, a través de Políticas, lineamientos, controles, requerimientos legales y buenas prácticas.

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera “Copia no Controlada”. La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.

	PROCESO: GESTIÓN TECNOLÓGICA		 ALCALDÍA MAYOR DE BOGOTÁ D.C. OFICINA Metro de Bogotá S.A.
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

CSIRT (Equipo de Respuesta a Incidentes de Seguridad)

El objetivo principal del CSIRT Gobierno, es ofrecer servicios proactivos, reactivos y de gestión de la seguridad básicos a todas las entidades del Estado, generando alertas y advertencias sobre amenazas y vulnerabilidades, realizando el tratamiento, análisis, respuesta y coordinación de incidentes, igualmente en el afianzamiento del conocimiento sobre seguridad, generando una cultura de seguridad digital en todos los funcionarios y encargados de seguridad digital. Cualquier tema relacionado con tratamiento de incidentes de seguridad, se debe reportar al correo csirtgob@mintic.gov.co.

colCERT (Grupo de Respuestas a Emergencias Cibernéticas de Colombia)

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. Cualquier tema relacionado con gestión y respuesta a incidentes cibernéticos, se debe reportar al correo contacto@colcert.gov.co.

7. ACTIVIDADES Y ENTREGABLES

Las actividades y entregables del presente documento fueron extraídas del Plan Estratégico de Tecnologías de la Información – PETI, fruto del ejercicio de Arquitectura Empresarial realizado en el 2021-2022 y que es actualizado anualmente en razón a los cambios de la estrategia del sector. En este sentido la Empresa Metro de Bogotá S.A, a través del diligenciamiento del instrumento del MSPI, y el seguimiento a la evolución de las tendencias en materia de tecnologías de la información, establece la hoja de ruta para los próximos cuatro años, realizando la implementación de buenas prácticas para el aseguramiento, control, monitoreo, mejoramiento y adquisición de servicios tecnológicos.

A continuación, se presentan las actividades para desarrollar y lograr fortalecer la Empresa, en materia de Seguridad de la Información para la vigencia 2022:

N°	Proceso/Actividades	Productos/Artefactos	Fecha inicial estimada	Fecha final estimada
1	Actualización de matriz de riesgos del proceso de TI con el direccionamiento de la Gerencia de Riesgos.	Matriz de riesgos del proceso de TI.	3 de enero de 2022	28 de febrero de 2022
2	Seguimiento a riesgos asociados a Seguridad digital y de la información.	Matriz de seguimiento de riesgos diligenciada.	1 de enero de 2022	31 de diciembre de 2022
3	Garantizar el cumplimiento de los lineamientos de seguridad de información por parte de ML1.	Actas, anexos y grabaciones de reuniones sostenidas con el concesionario ML1.	18 de noviembre de 2021	31 de mayo de 2022

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.

	PROCESO: GESTIÓN TECNOLÓGICA		
	PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-002	VERSIÓN: 01	

4	Elaboración del Plan de Apertura de Datos.	Plan Apertura de Datos.	26 de enero de 2022	30 de diciembre de 2022
5	Fortalecimiento de la infraestructura tecnológica de seguridad digital	Renovación licenciamiento firewall.	1 de julio de 2022	31 de diciembre de 2022
6		Fortalecimiento de las herramientas tecnológicas de seguridad.	1 de julio de 2022	31 de diciembre de 2022
7		Protección endpoints.	1 de septiembre de 2022	31 de diciembre de 2022
8		Otras actividades de implementación de la política de seguridad de información.	1 de junio de 2022	31 de diciembre de 2022
9		Adquisición certificados SSL.	1 de enero 2022	31 de marzo de 2022
10	Elaboración o actualización y ejecución del Plan de Sensibilización de Seguridad de la Información.	Plan de Sensibilización de Seguridad de la Información.	1 de marzo de 2022	30 de abril de 2022
11		Consultoría en Ingeniería Social y capacitaciones en seguridad digital.	1 de mayo de 2022	30 de noviembre de 2022
12	Elaboración del Plan de Recuperación de Desastres.	Plan de Recuperación de Desastres.	1 de abril de 2022	9 de diciembre de 2022

La EMB está comprometida con el medio ambiente; no imprima este documento. Si este documento se encuentra impreso se considera "Copia no Controlada". La versión vigente se encuentra publicada en aplicativo oficial de la Entidad.