PLAN OPERACIONAL DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción del cambio**
18/03/2022	01	Creación del documento.
Ver firma digital de aprobación del documento.	02	Actualización general del documento dando cumplimiento a lo establecido en el Decreto 612 de 2018.

Elaboró	Revisó	Aprobó	Aprobó SIG
Yuly Johana Rojas Idárraga Profesional Oficina de Tecnologías y Sistemas de Información	Juan Carlos Jiménez Aristizábal Jefe Oficina de Tecnologías y Sistemas de Información	Comité Institucional de Gestión y Desempeño Nota 1	Claudia Marcela Galvis Russi Representante de la Alta Dirección SIG

Firmado digitalmente por JUAN CARLOS JIMENEZ ARISTIZABAL

Diana Marcela Aponte – Oficina Asesora de Planeación

Nota 1: La aprobación del documento se da mediante sesión del Comité Institucional de Gestión y Desempeño - Acta No. 002 de 27 de enero de 2023.

CONTENIDO

1. INTRODUCCIÓN

Este documento expone las prioridades de implementación de los controles en relación a seguridad digital y 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 TI[2], 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 lo 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:

> "*La Política de Gobierno Digital será definida por el Ministerio de Tecnologías de Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC, conforme se describe a continuación:*
>
> *1. Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son:*
>
> *1.1. TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.*
>
> *1.2. TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.*

[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

2. Habilitadores Transversales de la Política de Gobierno Digital: 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."

A su vez, el numeral 3.2 del artículo 2.2.9.1.2.1 del Decreto 767 de 2022, respecto del habilitador de seguridad y privacidad de la información señala:

"(…)

3.2. Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad 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, disponibilidad y privacidad de los datos."

De esta forma, los componentes y habilitadores transversales son 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 actividades y 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 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.

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.

DECRETO 1072 DE 2022: 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.

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 27001:2013: 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.

BUENAS PRÁCTICAS: Acciones que se implementan para el cumplimiento de políticas y lineamientos y las cuales han dado resultados en otras personas, instituciones o ambientes.

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.

CIBERSEGURIDAD: Área que se enfoca en la protección de tecnologías de la información y activos de información.

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

CONTROL: Actividades de seguimiento y monitoreo que se llevan a cabo para mitigar un riesgo.

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

INCIDENTE DE SEGURIDAD DIGITAL: Violación y aprovechamiento de amenazas para explotar vulnerabilidades en plataformas tecnológicas o incumplimientos de las políticas y lineamientos definidos para la protección de los activos de información.

INGENIERÍA SOCIAL: Es una forma de ataque utilizado por un individuo que hace uso de técnicas psicológicas como la manipulación y habilidades sociales para obtener información valiosa y, de esta forma, lograr un objetivo trazado con buena o mala intención ingresar a sistemas o repositorios no autorizados, realizar sustracción de dinero o de información privada.

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

LINEAMIENTO: Directriz que describe la realización de ciertas actividades asociadas para cumplir políticas definidas previamente.

MINTIC: Ministerio de tecnologías de la información y las comunicaciones.

POLÍTICA: Manifiesto que presentan los objetivos a cumplir por una Entidad respecto a algún tema en particular.

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

RIESGO: se puede considerar como un agente de amenazas, ya sea humano o no humano, toma alguna acción, como identificar y explotar una vulnerabilidad, que ofrece un resultado inesperado y no deseado. Dichos resultados generan impactos negativos en la empresa.

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

SEGURIDAD DIGITAL: Corresponde a las actividades que se llevan a cabo para la protección de activos de información, redes, datos y dispositivos contra accesos no autorizados, evaluando amenazas, identificando vulnerabilidad y posibilidad de riesgo.

SENSIBILIZACIÓN: Presentar a un público objetivo la importancia de un tema en particular.

SGSI: Sistema de Gestión de Seguridad de la Información.

TECNOLOGÍAS DE LA INFORMACIÓN O TI: Aplicaciones, información e infraestructura requerida por una Entidad para apoyar el funcionamiento de los procesos y estrategias de la EMB S.A.

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 digital 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 digital y de la información.

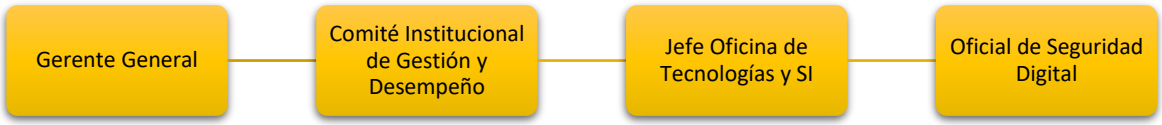
Comité Institucional de Gestión y Desempeño

La política de seguridad digital que contribuye con el desarrollo de las dimensiones de MIPG fue adoptada en la Resolución 738 de 2022 "*Por la cual se establece el reglamento de funcionamiento de Comité Institucional de Gestión y Desempeño de la Empresa Metro de Bogotá, conformación del equipo operativo SIG-MIPG y se dictan otras disposiciones*". 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 Digital 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 Digital" a través del manual de funciones y 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 Digital 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:



Fuente: Elaboración propia.

En consecuencia, el Oficial de Seguridad Digital, planea, diseña e implementa el SGSI de la Empresa, a través de Políticas, lineamientos, controles, requerimientos legales y buenas prácticas asociados con la seguridad digital de las Tecnologías de la Información (TI).

CSIRT (Equipo de Respuesta a Incidentes de Seguridad)

El objetivo principal del CSIRT Gobierno en cabeza del MinTIC, 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[3]. 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 en cabeza de MinTIC, tiene como responsabilidad central identificar infraestructuras críticas, gestionar sus riesgos de ciberseguridad, ofrecer a las empresas del sector público y privado información preventiva sobre amenazas y vulnerabilidades, apoyo y asesoría en la gestión de los incidentes de ciberseguridad, que garanticen la continuidad de las operaciones y servicios a la ciudadanía colombiana[4]. Cualquier tema relacionado con gestión y respuesta a incidentes cibernéticos, se debe reportar al correo contacto@colcert.gov.co.

7. ACTIVIDADES Y ENTREGABLES

Con el fin de dar cumplimiento y lograr el objetivo del presente plan, se establecen las siguientes actividades:

N°	Proceso/Actividades	Descripción	Productos/Artefactos	Fecha inicial estimada	Fecha final estimada
1	Seguimiento a riesgos asociados a Seguridad digital y de la información.	Ejecución del Plan de tratamiento de riesgos de seguridad digital y privacidad de la información, generando seguimiento y monitoreo a los controles definidos para la mitigación de riesgos.	Matriz de seguimiento de riesgos diligenciada.	1 de enero de 2023	31 de diciembre de 2023

[3] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/
[4] https://www.colcert.gov.co/800/w3-article-198657.html

N°	Proceso/Actividades	Descripción	Productos/Artefactos	Fecha inicial estimada	Fecha final estimada
2	Seguimiento al proyecto PLMB en el componente de TI y Seguridad Digital.	En el marco de la ejecución del proyecto de la Primera Línea del Metro de Bogotá se realizarán mesas de trabajo con los actores que intervienen en el proyecto, como ML1, Interventoría, PMO y EMB, con el fin de efectuar seguimiento al componente Tecnológico y de Seguridad Digital del proyecto PLMB.	Listados de asistencia, memorias de reunión, anexos y grabaciones de reuniones sostenidas.	1 de enero de 2023	31 de diciembre de 2023
3	Actualización y ejecución del Plan de Sensibilización de Seguridad de la Información	Realizar actualización del Plan de Sensibilización de Seguridad de la Información con el fin de incluir capacitaciones enfocadas en el fortalecimiento del conocimiento de la Política de Seguridad y Manejo de la Información de la EMB S.A.	Plan de Sensibilización de Seguridad de la Información.	1 de enero de 2023	31 de diciembre de 2023
4			Ejecución de pruebas de ingeniería social y capacitaciones en seguridad digital.	1 de enero de 2023	30 de marzo de 2023
5	Fortalecimiento de la infraestructura tecnológica de seguridad digital	Garantizar la actualización de certificados y licenciamiento que protegen los activos digitales de la Entidad como el portal web, sistemas de información, datos y red.	Adquisición certificado SSL para portal metrodebogota.gov.co	1 de febrero de 2023	31 de mayo de 2023
6			Renovación licenciamiento firewall y plataforma de logs y monitoreo de eventos.	1 de julio de 2023	31 de diciembre de 2023
7	Actualización de la política de seguridad digital y manejo de la información	De acuerdo con la Norma NTC-ISO/IEC 27001 Y 27002, así como los lineamientos impartidos por MinTIC, actualizar la política digital y manejo de la información implementando las políticas determinadas en la Norma. .	Política de Seguridad y manejo de la información.	1 de abril de 2023	31 de diciembre de 2023
8	Análisis del resultado de pruebas de vulnerabilidad	Generar mesas de trabajo al interior de la OTI y determinar las actividades a realizar para cerrar brechas de acuerdo con el resultado de análisis de vulnerabilidades.	Plan de trabajo de cierre de brechas.	15 de abril de 2023	30 de junio de 2023

N°	Proceso/Actividades	Descripción	Productos/Artefactos	Fecha inicial estimada	Fecha final estimada
9	Elaboración del Plan de Recuperación de Desastres	Construcción de la estrategia que se seguirá para restablecer los servicios de TI, conocidos como el Hardware y Software, después de haber sufrido una afectación por: una catástrofe natural o epidemiológica, falla masiva eléctrica (apagones de luz, fallas en el edificio, fallas de hardware), daño premeditado, (secuestro de la información, ransomware, hackeos, robo de datos), ataque de cualquier tipo el cual atente contra la continuidad del negocio.	Plan de Recuperación de Desastres.	1 de junio de 2023	30 de abril de 2024
10	Actualización activos de información digital	Implementar las acciones descritas en el MN-GR-001 para la identificación de activos de información digital.	Matriz de activos de información digital diligenciada.	1 de julio de 2023	30 de abril de 2024
11	Planear y ejecutar la semana de seguridad digital en la EMB	Teniendo en cuenta que el 30 de noviembre es el día internacional de la seguridad digital/informática, se programarán y ejecutarán actividades para llevar a cabo la realización de la semana de la seguridad digital al interior de la EMB en noviembre.	Cronograma con temáticas, fechas e invitados.	1 de octubre de 2023	31 de diciembre de 2023

ANEXO: CRONOGRAMA

N°	Proceso/Actividades	Productos/Artefactos	2023												2024			
			ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR
1	Seguimiento a riesgos asociados a Seguridad digital y de la información.	Matriz de seguimiento de riesgos diligenciada.																
2	Seguimiento al proyecto PLMB en el componente de TI y Seguridad Digital.	Listados de asistencia, memorias de reunión, anexos y grabaciones de reuniones sostenidas.																
3	Actualización y ejecución del Plan de Sensibilización de Seguridad de la Información	Plan de Sensibilización de Seguridad de la Información.																
4		Ejecución de pruebas de ingeniería social y capacitaciones en seguridad digital.																
5	Fortalecimiento de la infraestructura tecnológica de seguridad digital	Adquisición certificado SSL para portal metrodebogota.gov.co																
6		Renovación licenciamiento firewall y plataforma de logs y monitoreo de eventos.																
7	Actualización de la política de seguridad digital y manejo de la información	Política de Seguridad y manejo de la información.																
8	Análisis del resultado de pruebas de vulnerabilidad	Plan de trabajo de cierre de brechas.																
9	Elaboración del Plan de Recuperación de Desastres	Plan de Recuperación de Desastres.																
10	Actualización activos de información digital	Matriz de activos de información digital diligenciada.																
11	Planear y ejecutar la semana de seguridad digital en la EMB	Cronograma con temáticas, fechas e invitados.																