

	PROCESO: GESTIÓN TECNOLÓGICA		
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS		
Fecha	Versión	Descripción del cambio
18703/2022	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-005_V.01 a GT-DR-003_V.01), se realiza modificación general al documento.
Ver firma digital de aprobación del documento.	02	Actualización del documento de acuerdo con el Decreto 612 de 2018.

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

DR Daniela Roza Rodríguez – 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 20

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVO	3
3. ALCANCE.....	3
4. DEFINICIONES, SÍMBOLOS Y ABREVIATURAS	3
5. GENERALIDADES.....	5
6. METODOLOGÍA PARA EL TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	7
7. PLAN DE TRATAMIENTO	12

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

1. INTRODUCCIÓN

De acuerdo con lo establecido en la Guía No. 7 de MINTIC correspondiente a la Gestión de Riesgos de Seguridad y Privacidad de la Información, la cual establece los lineamientos para gestionar los riesgos de seguridad de la información integrando la Metodología de Riesgos del DAFP, se desarrolló al interior de la EMB S.A el Plan de Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información con el fin de dar cumplimiento a la Guía.

Con el compromiso de la alta y media dirección de la entidad se conforma el equipo interdisciplinario liderado por el Gerente de Riesgos como directivo de primer nivel quien es parte del MECI de la entidad encargado de los procesos correspondientes a la administración de riesgos.

El presente documento integra las etapas y elementos establecidos en la Guía para el tratamiento de los riesgos de Seguridad de la información, así como los criterios para su evaluación, alcance, límites valoración de controles, plan de implementación y los demás a que haya lugar.

2. OBJETIVO

Desarrollar las etapas del MSPI e implementarlas al interior de la Empresa Metro de Bogotá S.A, con el fin de realizar una correcta identificación, análisis, valoración, monitoreo y seguimiento de controles.

3. ALCANCE

Este plan es aplicable a todos los servidores, contratistas y procesos de la Empresa Metro de Bogotá S.A, de la misma manera, el plan inicia con la identificación del contexto estratégico organizacional hasta el monitoreo y revisión del proceso para la administración del riesgo.

4. DEFINICIONES, SÍMBOLOS Y ABREVIATURAS

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

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.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

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

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo es evaluada.

Control: Medida que modifica el riesgo.

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

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

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

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesas de trabajo, en las cuales se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: “Proceso para modificar el riesgo” (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

5. GENERALIDADES

La Empresa Metro de Bogotá S.A. - EMB S.A., es una sociedad por acciones del orden Distrital, descentralizada, con personería jurídica, autonomía administrativa, financiera y presupuestal, patrimonio propio, vinculada a la Secretaría Distrital de Movilidad, con régimen jurídico de empresa industrial y comercial del Estado, vinculada al sector movilidad, cuyo objeto principal se encuentra definido en el artículo 2º del Acuerdo Distrital No. 642 del 12 de mayo de 2016, "Por el cual se autoriza al Alcalde Mayor en representación del Distrito Capital para participar, juntamente con otras entidades descentralizadas del orden Distrital, en la constitución de la Empresa Metro de Bogotá S.A., se modifican parcialmente los Acuerdos Distritales 118 de 2003 y 257 de 2006, se autorizan compromisos presupuestales y se dictan otras disposiciones en relación con el Sistema Integrado de Transporte Público de Bogotá", así:

“Corresponde a la EMB realizar 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.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

También 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 criterios de sostenibilidad. Todo lo anterior, en las condiciones que señalen las normas vigentes, autoridades competentes y sus propios estatutos.”.

La EMB consciente de la complejidad de sus operaciones, del cumplimiento de su misión y visión, considera importante, relevante y fundamental adoptar de manera integral políticas para una adecuada gestión de riesgos y efectuar su implementación, siendo este un objetivo de la Alta Dirección.

Son funciones de la Gerencia de Riesgos las siguientes:

- **Acuerdo 007 de 2021, Artículo 21°.** - **Gerencia de Riesgos.** *“Son funciones de la Gerencia de Riesgos las siguientes:*
 - a) Definir la estructura y el modelo de gobierno de riesgos institucionales, financieros y de los proyectos de la entidad, contribuyendo a la apropiación por parte de la alta gerencia y estableciendo una asignación clara de responsabilidades entre las unidades funcionales y de control.*
 - b) Definir, desarrollar, documentar, implementar, articular, capacitar y socializar las políticas y metodologías para la administración de riesgos de la Empresa Metro de Bogotá, conforme al marco de referencia de las mejores prácticas y normatividad vigente.*
 - c) Establecer e implementar los mecanismos adecuados de control y gestión de riesgos conforme a la estructura, los proyectos y perfil de riesgos.*
 - d) Orientar a todas las dependencias de la EMB en el despliegue de las metodologías para la gestión de riesgos, la elaboración de las matrices de riesgos y los planes de mitigación de riesgos.”*

De conformidad con el documento “Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas” el cual para la EMB se encuentra incorporado en el Manual para la gestión de riesgos institucionales en la EMB (versión vigente) con código SIG: GR-MN-001 liderado por la Gerencia de Riesgos.

En el marco del Modelo Integrado de Planeación y Gestión – MIPG -, en la Dimensión de Control Interno, el MECL particularmente en su componente de Gestión de Riesgos es desarrollado por la Gerencia de Riesgos (Res. 111 de 2020).

Este documento pretende orientar a los servidores públicos, trabajadores oficiales y contratistas de la EMB S.A en la identificación, análisis, valoración, monitoreo y revisión de los riesgos de seguridad y privacidad de la información.

Así mismo, se establecen controles y responsabilidades para la administración de los riesgos que permitan brindar seguridad para responder y controlar los posibles acontecimientos potenciales o aquellos que se pueden llegar a presentar dentro de la operación de la EMB S.A.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

6. METODOLOGÍA PARA EL TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La EMB S.A tomará como referente los parámetros establecidos por el Departamento Administrativo de la Función Pública DAFP y el Ministerio de Tecnologías de la Información y Comunicaciones MINTIC, de la Guía para la administración del riesgo y el diseño de controles en entidades públicas la cual articula los riesgos de gestión, corrupción y seguridad digital y la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información Guía No. 7 del MINTIC.

Proceso para la administración del riesgo

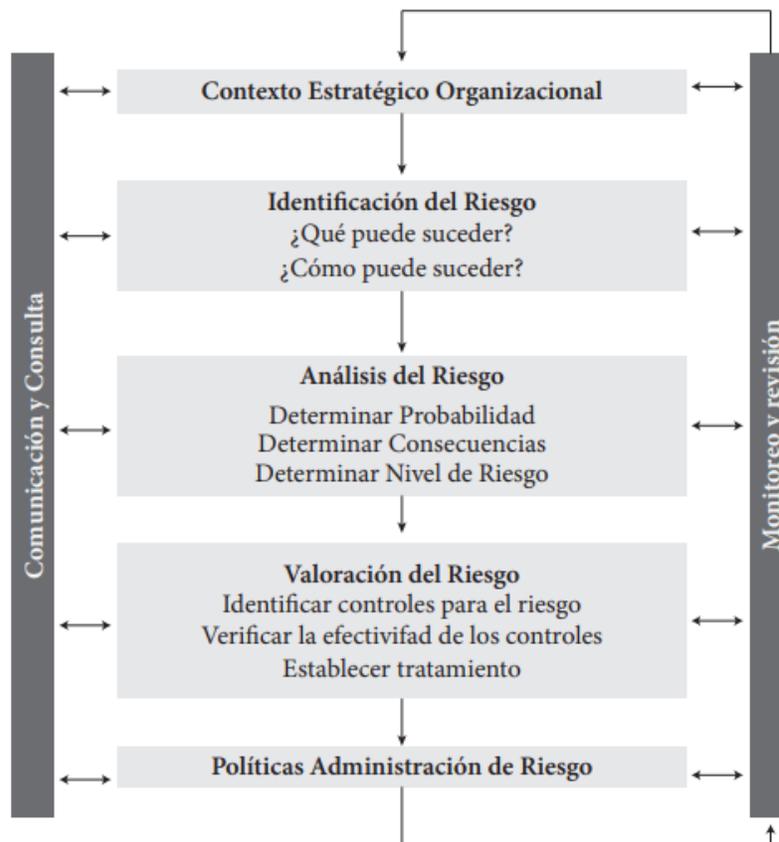


Figura 1. Proceso para la administración del riesgo
Fuente: Guía para la Administración del Riesgo-DAFP.

<https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba>

6.1. Antes de iniciar con el plan de tratamiento

El desarrollo del plan de tratamiento de riesgos de seguridad digital y privacidad de la información se debe encontrar articulado y alineado con el marco de referencia de la entidad, donde se tenga claridad frente a los objetivos institucionales de la Empresa Metro de Bogotá S.A.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

6.1.1. Contexto estratégico organizacional

Misión: Nuestro propósito como Empresa Metro de Bogotá es transformar positivamente la movilidad del Distrito Capital mediante la implementación y operación del modo ferroviario del SITP; con conexión a las redes de integración regional, aportando al desarrollo y renovación urbana de la ciudad, con el fin de generar acceso a oportunidades urbanas y mejorar la calidad de vida de los ciudadanos.

Visión: En el año 2028, con la entrada en operación de la PLMB, la Empresa será reconocida como ejemplo de gestión de movilidad sostenible, segura, confiable, eficiente y con altos estándares tecnológicos. Se habrá definido la expansión de la PLMB, conectándose con el SITP y fortaleciendo la consolidación del modo férreo regional. La EMB, será un referente de cultura, valores y motivo de orgullo y apropiación ciudadana, por su contribución a la transformación positiva de la capital. Adicionalmente, será reconocida en América por la generación de otras fuentes de financiación que contribuyan a su sostenibilidad en el tiempo.

Planeación Estratégica: Alinear la Entidad en torno a las prioridades de política pública e institucional en el marco del Plan Desarrollo Distrital y el Plan Sectorial, a través de directrices y lineamientos necesarios para elaborar y hacer seguimiento a los planes de inversión conforme a lo establecido en la misión, visión y objetivos estratégicos de la Entidad, apalancado en el plan de anual de adquisiciones.

Gestión de Riesgos: Gestionar los riesgos de la entidad de manera permanente, con la participación de los grupos de valor y partes interesadas de la EMB, por medio del uso de herramientas y metodologías disponibles, con el fin de administrar y fomentar la cultura de la gestión de riesgos con los recursos disponibles.

Gestión de Tecnología: Transformar los procesos de negocio con tecnología digital, buscando la alineación del negocio e impulsar las estrategias de la empresa Metro de Bogotá, a través de la creación, adquisición, implementación y gestión de servicios eficientes y rentables, y a la reducción de los riesgos asociados a dichos servicios, mejorando la gestión, apalancado en el plan anual de adquisiciones de la vigencia durante el plan de desarrollo distrital vigente.

6.1.2. Proceso para la administración del riesgo

Los lineamientos establecidos para la administración de los riesgos se encuentran definidos en el documento GR-MN-001 Manual para la gestión de riesgos institucionales en la EMB, el cual se encuentra para consulta en el Sistema Integrado de Gestión, este documento se encuentra alineado con la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP.

Así mismo, los procesos de la entidad que salvaguardan la seguridad y privacidad de la información cuentan con la identificación, valoración y establecimiento de controles e indicadores en las matrices de riesgos, las cuales se encuentran publicadas en el Sistema Integrado de Gestión.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

Este documento se enfoca en las actividades propias de los procesos para dar cumplimiento a lo establecido en las matrices de riesgos, para así prevenir, mitigar o trasladar los riesgos según corresponda.

6.2. Plan de tratamiento de riesgos de seguridad y privacidad de la información

6.2.1. Contexto Estratégico

La empresa Metro de Bogotá S.A. cuenta con activos de información que deben ser protegidos y salvaguardados de posibles amenazas que puedan atentar su integridad, disponibilidad y confiabilidad, para ello a continuación se presenta la Matriz DOFA:

(D) Debilidades (factores negativos internos)	(F) Fortalezas (factores positivos internos)
El respaldo con el que cuenta actualmente la infraestructura tecnológica aún no es suficiente.	Uso eficiente de los recursos de TI.
Mal uso, errores funcionales y operativos por parte de los usuarios autorizados no administradores (Compromiso de funciones).	Políticas y lineamientos enfocados en el proceso de Gestión de TI.
Fallas en los controles de acceso de los usuarios a la información (Compromiso de funciones).	Con las herramientas disponibles se realiza monitoreo preventivo a parte de la infraestructura tecnológica.
Controles del Modelo de seguridad y privacidad de la Información que no se estén cumpliendo en los sistemas de información habilitados.	Recurso humano con conocimiento y experiencia en la administración de los recursos tecnológicos.
Fallas técnicas imprevistas de la infraestructura tecnológica (Fallas técnicas).	Recurso humano con conocimiento y experiencia en gobierno digital, seguridad digital y de la información digital.
Falta de continua capacitación en el buen manejo de las aplicaciones existentes y de las nuevas para obtener su mayor provecho.	Habilidades de los miembros del equipo para la transformación digital.
Errores en el almacenamiento de información por parte de los dueños de la información.	Actitud de servicio al cliente por parte del equipo de OTI.
Los servidores de la OTI realicen actividades operativas y funcionales pertenecientes a otros procesos.	Equipo humano que diseña y propone proyectos de desarrollo de aplicaciones basados en arquitecturas estándares que permiten su usabilidad, accesibilidad, mantenibilidad, escalabilidad y fácil integración e interoperabilidad con otras aplicaciones.
Falta de presupuesto para suplir las necesidades estratégicas de las áreas solicitadas a la OTI.	Capacidad para definir políticas y procedimientos que mejoren y transformen de manera eficiente el proceso de gestión de TI.
Información de la entidad en equipos personales de los servidores públicos.	Conocimiento del equipo de OTI en los procesos internos y de interacción con entes externos.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

**(O) Oportunidades
(factores positivos externos)**

**(A) Amenazas
(factores negativos externos)**

Transferencia de conocimiento por parte de los proveedores, Entidades del sector TIC y del Distrito que fortalecen los conocimientos en el uso y apropiación de las herramientas tecnológicas.	Compromiso de la información.
Potenciar las actuales tecnologías e implementar nuevas a partir de las que se encuentran disponibles en el mercado.	Fallas técnicas en los servicios contratados con terceros.
Retroalimentación de los ciudadanos y usuarios internos que pueden convertirse en soluciones tecnológicas.	Ingresos no autorizados por parte de un externo.
Apropiación de conocimientos tecnológicos de los terceros con los que interactúa la EMB.	Eventos naturales.
Adopción e implementación de los lineamientos del MinTIC para estandarizar y lograr la transformación digital, el diseño inclusivo, el uso y apropiación de las TIC para impulsar y cumplir con los objetivos de la EMB.	Pérdida de los servicios esenciales.
A partir de los requerimientos de la Resolución 1519 de 2020 del MINTIC se identifican oportunidades de mejora para el diseño, desarrollo e implementación de un Portal web.	Daños en las instalaciones donde se ubica el centro de cómputo que afecten la operación y funcionamiento de la infraestructura tecnológica.
	Alto volumen de normatividad vigente por adoptar e implementar que afecte el funcionamiento y la estrategia de la Oficina de TI de la EMB.
	Cambio en los lineamientos definidos por las entidades del sector TIC que impacten el proceso de gestión de TI.
	Recortes presupuestales que afecten la adquisición y/o contratación de prestación de servicios de TI.

6.2.2. Tipología de activos

Tipo de activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD, unidades USB) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores). Teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.

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. MOVILIDAD Metro de Bogotá S.A.
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

Hardware	Equipos físicos de cómputo y de comunicaciones como servidores, biométricos que por su criticidad son considerados activos de información.
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, gestor documental, ERP, Portales organizacionales, Aplicaciones entre otros (pueden estar compuestos por hardware y software).
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante; puede ser la imagen corporativa, reputación o el 'good will', entre otros.
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

6.2.3. Clasificación de la información

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.

6.2.4. Clasificación de la información Valoración del activo (determinar la criticidad del activo)

La escala de valoración utilizada por la Empresa Metro de Bogotá para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia para el proceso, será Alta, Medio y Baja.

Tipo de clasificación
Alta
Media
Baja

Una vez se realiza la identificación de los activos, la Empresa Metro de Bogotá gestionará los riesgos en todos los activos del inventario, de acuerdo con lo consignado en este documento.

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN		
	CÓDIGO: GT-DR-003	VERSIÓN: 02	

7. PLAN DE TRATAMIENTO

Descripción del Riesgo	Nivel Probabilidad Inherente	% Prob	Indicador del riesgo	No. Control	Descripción del control	Responsable del control	Indicador del control
GT-RI-001 Posibilidad de Impacto reputacional y/o económico generado por la pérdida de confidencialidad de la información contenida en los repositorios internos y externos y en los sistemas de información causada por un compromiso de la información, mal funcionamiento del software, uso no autorizado del equipo, abuso de derechos y/o	Muy alta	100%	(No. de amenazas que no fueron neutralizadas / No total de amenazas) * 100 Nota: Este porcentaje no debería ser superior al 1%	GT-C1	Los profesionales de infraestructura y soporte de TI reciben las solicitudes de creación de usuarios remitidas por los Jefes de área o Supervisores, de forma que asignan los permisos correspondientes o se escala a los Líderes Funcionales de los aplicativos para continuar el trámite, actualizando en todo caso la Matriz de roles y permisos. Lo anterior con el propósito de evitar el acceso no autorizado a los repositorios de información de la entidad.	Los profesionales de infraestructura y soporte de TI	(No. de solicitudes atendidas que fueron aprobadas por el dueño de proceso / No. de solicitudes recibidas que fueron aprobadas por el dueño de proceso)*100
				GT-C2	Los profesionales del Equipo de Servicios Tecnológicos realizan seguimiento a las alertas automáticas generadas por la Plataforma de Monitoreo de Seguridad Perimetral. El sistema de manera automática bloquea y neutraliza los ataques cibernéticos externos, generando la alerta correspondiente. Cuando se generan estas alertas el sistema reporta de manera automática al Proveedor para que se actualice el software de protección en caso que se requiera.	Los profesionales del Equipo de Servicios Tecnológicos	(No. de ataques solucionados / No. de ataques recibidos)* 100

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y
PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: GT-DR-003

VERSIÓN: 02



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
MOVILIDAD
Metro de Bogotá S.A.

falsificación de derechos				GT-C3	Los profesionales del Equipo de Servicios Tecnológicos realizan seguimiento a las notificaciones de actualización de software que genera cada plataforma tecnológica. De tal manera que se programa la ejecución de las actualizaciones correspondientes.	Los profesionales del Equipo de Servicios Tecnológicos	(No. de actualizaciones realizadas / No. de actualizaciones recibidas en el periodo)*100
GT-RI-002 Posibilidad de Impacto reputacional y/o económico generado por la pérdida de integridad de la información contenida en los repositorios internos y externos y en los sistemas de información causado por corrupción de los datos, procesamiento ilegal de datos, fallas técnicas, error en el uso/abuso de	Muy alta	100%	No. total de reportes en que no se haya podido restaurar la información que haya presentado pérdida de integridad	GT-C1	Los profesionales de infraestructura y soporte de TI reciben las solicitudes de creación de usuarios remitidas por los Jefes de área o Supervisores, de forma que asignan los permisos correspondientes o se escala a los Líderes Funcionales de los aplicativos para continuar el trámite, actualizando en todo caso la Matriz de roles y permisos. Lo anterior con el propósito de evitar el acceso no autorizado a los repositorios de información de la entidad.	Los profesionales de infraestructura y soporte de TI	(No. de solicitudes atendidas que fueron aprobadas por el dueño de proceso / No. de solicitudes recibidas que fueron aprobadas por el dueño de proceso)*100
				GT-C4	Los profesionales de infraestructura y soporte de TI realizan seguimiento mensual a la generación de los backups automáticos realizados por el proveedor, dejando evidencia en el informe de infraestructura y gestión, con el propósito de evidenciar que los backups se hayan realizado. En caso de desviaciones se creará el caso con el proveedor para la revisión de las inconsistencias.	Los profesionales de infraestructura y soporte de TI	(No. de Backups realizados por el proveedor / No. de Backups programados en el periodo) * 100

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y
PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: GT-DR-003

VERSIÓN: 02



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
MOVILIDAD
Metro de Bogotá S.A.

derechos y/o falsificación de derechos				GT-C5	Los profesionales de infraestructura y soporte de TI realizan seguimiento a los backups automáticos que se generan a diario para el servidor del Data Center, dejando evidencia de su realización en el Informe de infraestructura y gestión. En caso que se detecte en el Log que se presentó una falla en la realización del backup, se proceden a ejecutar las copias de seguridad para corregir los errores que se hayan presentado.	Los profesionales de infraestructura y soporte de TI	(No. de Backups automáticos diarios realizados / No. de Backups automáticos programados en el periodo) * 100
				GT-C6	Los profesionales de infraestructura y soporte de TI realizan seguimiento al Cronograma de mantenimiento preventivo establecido con el proveedor para la realización de los mantenimientos a la UPS, servidores, equipos de cómputo, aire acondicionado; dejando evidencia de su realización en el Informe de infraestructura y gestión. Lo anterior, con el propósito de prevenir futuros daños, ya sean a nivel de Hardware, Software o de un componente electrónico.	Los profesionales de infraestructura y soporte de TI	(No. de mantenimientos preventivos ejecutados por el proveedor / No. de mantenimientos programados en el periodo) * 100
				GT-C7	Los profesionales de infraestructura y soporte de TI reportan los diferentes fallos en los dispositivos tecnológicos a los proveedores de servicios, con el fin de que se realicen los respectivos mantenimientos correctivos para resolver las incidencias presentadas; dejando evidencia de su realización en el Informe de infraestructura y	Los profesionales de infraestructura y soporte de TI	No. de fallos atendidos por los proveedores de servicios / No. de fallos presentados) * 100

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y
PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: GT-DR-003

VERSIÓN: 02



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
MOVILIDAD
Metro de Bogotá S.A.

					gestión. El proveedor presenta un reporte, el cual es validado con el fin de evidenciar si se resolvieron las diferentes incidencias.		
GT-RI-003 Posibilidad de Impacto reputacional y/o económico generado por la pérdida de disponibilidad de la información contenida en los repositorios internos y externos y en los sistemas de información causada por daños físicos, eventos naturales, pérdida de los servicios esenciales, y/o uso no autorizado del equipo	Muy alta	100%	No. de veces que se presentó pérdida de disponibilidad de la información incumpliendo o los ANS establecidos	GT-C8	Los profesionales de infraestructura y soporte de TI remiten el Inventario de equipos o las modificaciones a éste, a la Gerencia Administrativa y de Abastecimiento (GAA) para efectos de actualización del inventario, información que la GAA remite a la Gerencia de Riesgos para la adquisición de la póliza Todo Riesgo Daño Material, de tal forma que se incluyan los amparos necesarios para cubrir cualquier eventualidad que pueda afectar la infraestructura de TI (equipos de cómputo, equipos eléctricos y electrónicos, reinstalación y recuperación del software, reposición de las licencias, infraestructura física, entre otros). Así mismo, se debe reportar a la Gerencia de Riesgos los siniestros ocurridos, de conformidad con lo establecido en el procedimiento GR-PR-006.	Los profesionales de infraestructura y soporte de TI	(No. de siniestros reportados / No. de siniestros ocurridos)* 100 No. de actualizaciones del inventario remitidas a la GAA en el periodo / No. de actualizaciones de inventario tecnológico ocurridas en el período)* 100
				GT-C9	Los profesionales de infraestructura y soporte de TI realizan seguimiento mensual a la capacidad, disponibilidad de los servicios de TI y conectividad de acuerdo con los ANS establecidos con el proveedor. En caso que se detecte algún fallo o degradación del servicio se reporta al proveedor para la solución de las incidencias.	Los profesionales de infraestructura y soporte de TI	(No. de servicios de TI y de conectividad que presentaron indisponibilidad con relación a los ANS establecidos / Total de servicios de TI y de conectividad)* 100

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 DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL Y
PRIVACIDAD DE LA INFORMACIÓN

CÓDIGO: GT-DR-003

VERSIÓN: 02



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
MOVILIDAD
Metro de Bogotá S.A.

				GT-C10	Los profesionales de infraestructura y soporte de TI realizan seguimiento al Consolidado de los contratos de licenciamiento de software verificando su estado, con el fin de gestionar la renovación del contrato del servicio de mantenimiento y soporte de software de las licencias de acuerdo con el vencimiento de cada una, o en caso de requerirse la adquisición de licencias gestionando el respectivo proceso de contratación. Actualizando el Consolidado de los contratos de licenciamiento de software, cada vez que se adquiera o renueve una licencia, o se haya dado de baja en caso que el software haya entrado en desuso.	Los profesionales de infraestructura y soporte de TI	No. de licenciamientos renovados /No. Total de licencias que se vencen en el periodo) *100
--	--	--	--	--------	--	--	--

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.