MOVILIDAD FUTURA

Seguridad Digital

Agosto 2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Que la Constitución Política de Colombia adopto los principios de la función administrativa, eliminación del control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno, Que la Ley 1474 de 2011 incorporo a la legislación nacional el Estatuto Anticorrupción, 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. El Modelo Integrado de Planeación y Gestión (MIPG) compilo los sistemas de gestión de calidad de la Ley 872 de 2003 y de Desarrollo Administrativo de que trataba la Ley 489 de 1998. Desarrollado mediante la Ley 1753 de 2015 a partir de la cual se dispone la fusión del Sistema de Desarrollo Administrativo y el de Gestión de Calidad y su articulación con el de Control Interno, el cual fue reglamentado mediante decreto 1083 de 2015 que a su vez fue modificado por el decreto 1499 de 2017.

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1499 de 2017.

MIPG busca mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento para la difusión de información confiable y oportuna; es uno de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

Para lograr alinear a través de la presente guía se definen las estrategias y mecanismos mediante los cuales se desarrolla e implementa la Política de Seguridad Digital en el marco del Modelo Integrado de Planeación y Gestión MIPG.

En Movilidad Futura S.A.S., la información es el activo más preciado, por tanto, este ha tomado todas las precauciones necesarias, para mantenerla y preservarla, para ello la entidad ha venido desarrollando y evolucionando su modelo de seguridad de la información soportado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad; así como adoptando buenas prácticas en cuanto a la gestión y administración de las TI.

De acuerdo con la política de gobierno digital, liderada por el Ministerio de las Tecnologías y las Comunicaciones - Min TIC, cuyo objetivo es garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un estado más participativo, más eficiente y más transparente, Movilidad Futura S.A.S., a través del Subproceso de Tecnología, ha venido realizando la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea –GEL, para diseñar, adoptar y promover las políticas de seguridad digital en la entidad.

2. OBJETIVO

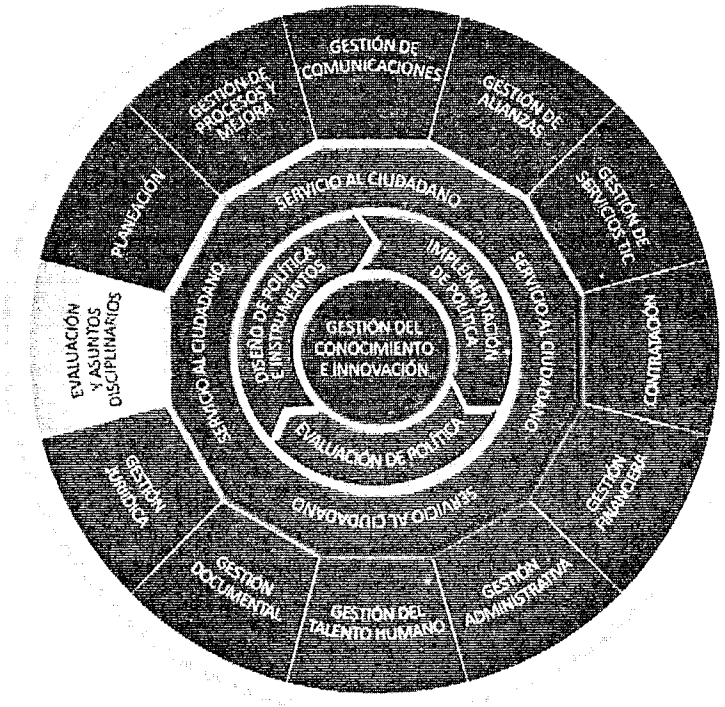
A través de la presente guía se definen las estrategias de implementación de la política de Fortalecimiento Institucional y simplificación de procesos en Movilidad Futura S.A.S., entregando los lineamientos para la optimización de sus procesos, el incremento de la productividad y la generación del valor público.

Movilidad Futura S.A.S. se compromete a formalizar y garantizar los tres (3) pilares fundamentales de la seguridad de la información - confidencialidad, integridad y disponibilidad -, gestionando y controlando la implementación de la seguridad digital al interior de la entidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, y la definición de controles para la mitigación del riesgo, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la información, el cual está a cargo del subproceso de tecnología.

Según lo que se establece en la resolución 00059 de noviembre 11 del 2020, en el **Plan Estratégico 2020 – 2023 Creemos en el futuro de Popayán:** Movilidad futura S.A.S., a partir de las necesidades de gestión, se compromete a adecuar el diseño organizacional para hacerlo eficiente, a trabajar por los procesos para optimizar los recursos físicos, de manera tal que se mejore la prestación de los servicios tecnológicos y se garantice una buena seguridad para la información que se obtiene o genera en cada proceso.

3. ALCANCE

A través de la presente guía se definen las estrategias y mecanismos mediante las cuales se desarrolla e implementa la POLÍTICA DE SEGURIDAD DIGITAL, cuya responsabilidad, se encuentra inmersa en el proceso de Gestión Administrativa, específicamente en el subproceso de tecnología, para la entidad de Movilidad Futura S.A.S.



4. DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

Con la política de Seguridad Digital se pretende fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades laborales o socioeconómicas frente al entorno digital, en un marco de cooperación, colaboración y asistencia; lo que a su vez impulsará una mayor prosperidad económica y social para la entidad.

Movilidad Futura S.A.S. se compromete a formalizar y garantizar los tres (3) pilares fundamentales de la seguridad de la información - confidencialidad, integridad y disponibilidad -, gestionando y controlando la implementación de la seguridad digital al interior de la entidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, y la definición de controles para la mitigación del riesgo, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la información que está a cargo del subproceso de tecnología.

5. MARCO DE REFERENCIA

Constitución Política de Colombia 1991. 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 23 de 1982. 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.

Ley 594 de 2000. Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

Ley 603 del 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la **Ley 603 de 2000** obliga a las empresas a declarar si los problemas de software son o no legales.

Ley 962 de 2005. Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

Ley 1755 2015. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Título II Capítulo I.

Conpes 3854 2016. Política Nacional de Seguridad Digital

Decreto 2364 2012 Firma electrónica

Decreto 2609 2012 Expediente electrónico 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 1078 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

6. DEFINICIONES

ACTIVO DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

LINEAMIENTOS: Directriz o disposición establecida por el Ministerio TIC, que debe ser implementada por las entidades públicas para el desarrollo de la Política de Gobierno Digital y se desarrolla a través de estándares, guías, recomendaciones o buenas prácticas.

ESTÁNDAR: Es el conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Un estándar se construye a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular, implican uniformidad y normalización y es de obligatorio cumplimiento.

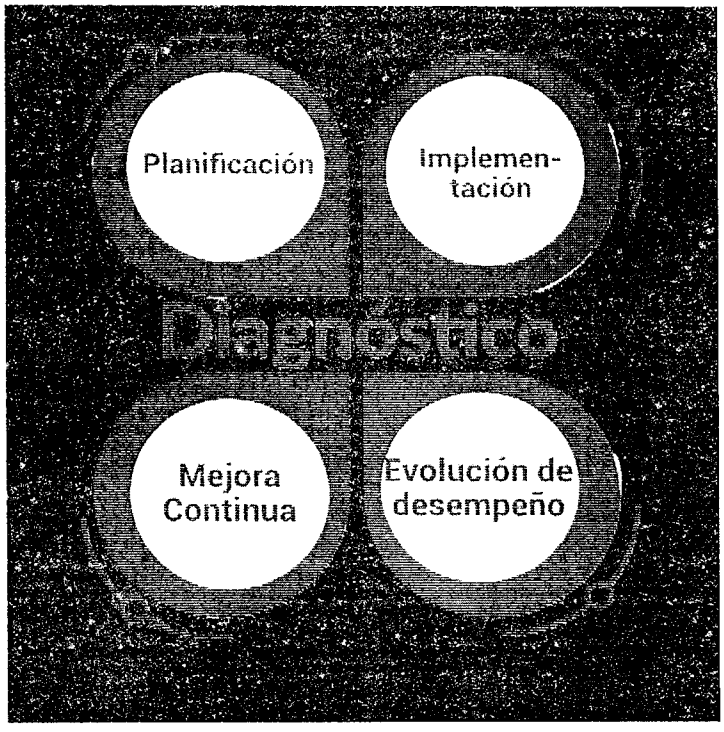
ARQUITECTURA: Este habilitador busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar

SEGURIDAD DE LA INFORMACIÓN: Este habilitador busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales.

7. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL.

El Comité Institucional de Gestión y Desempeño de Movilidad Futura S.A.S., con el objeto de articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política de Gobierno Digital designa como responsable de la Seguridad Digital y de la Seguridad de la Información en la entidad, al Proceso Administrativo.

La formalización de la política por parte de Movilidad Futura S.A.S., se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital dispuesto por el Min TIC. Se dará cumplimiento a las actividades relacionadas en el plan de acción.



Categoría	Actividades de Gestión	Estrategias o mecanismos	Política con la que Interactúa	Área responsable	Periodicidad
Gestión de Servicios TIC	Diseño, definición o actualización de los documentos y controles.	Plan de Seguridad y Privacidad de la Información	N/A	Administrativa Tecnología	Anual
	Diseño, definición o actualización de la gestión de levantamiento de activos de información.	Inventario de activos de información		Administrativa Tecnología	Anual
	Diseño, definición o actualización de la gestión de los riegos de seguridad digital	Riesgos de información		Administrativa Tecnología	Anual

ELABORADO POR	REVISADO POR	APROBADO POR
MAURICIO TROCHEZ TUNUBALA	JAIRO ERNESTO DUQUE ROSERO	ROBERTH DUVALL HORMIGA TIMANÁ
Contratista Apoyo Planeación	Contratista Líder Planeación	Gerente

Revisó: EDUAR TUQUERRES RUIZ – Contratista Apoyo Tecnología
Reviso: Víctor Gómez – Contratista Líder Jurídico
Proyectó: MAURICIO TROCHEZ TUNUBALA – Apoyo Planeación