



PLANEACIÓN	Código: Plnst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025



Alcaldía de Popayán



POLÍTICA DE SEGURIDAD DIGITAL

Octubre 2025

Carrera 9 N°. 62N-47. Bellavista - Popayán

Teléfono: 8205898

www.movilidadfutura.gov.co - servicioalciudadano@movilidadfutura.gov.co

Nit:900323358-2

PLANEACIÓN	Código: PInst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN
2. OBJETIVO GENERAL
 - 2.1. OBJETIVOS ESPECIFICOS
3. ALCANCE
4. DESCRIPCIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL
5. MARCO DE REFERENCIA
6. DEFINICIONES
7. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL
8. ACCIONES PARA MANTENER LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL
9. RESULTADOS DE MEDICIÓN DE DESEMPEÑO INSTITUCIONAL

PLANEACIÓN	Código: Pinat-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

1. INTRODUCCIÓN

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 489 de 1998. Desarrollando mediante la ley 1753 de 2015 a partir de la cual se dispone la función del sistema del Desarrollo Administrativo y el de Gestión de la 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 del 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 resuelven las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1499 del 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 de la parte pública 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 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 SAS, la información es el activo mas 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 dos pilares fundamentales tales como: Integridad y disponibilidad; así como adoptando buenas prácticas en cuanto a la gestión y administración de la TIC.

De acuerdo a la Política de Gobierno Digital, liderada por el ministerio de las Tecnologías de las Comunicaciones Min TIC, cuyo objetivo es garantizar el máximo aprovechamiento

PLANEACIÓN	Código: Plnst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

de las tecnologías de la información y las comunicaciones con el fin de contribuir con la construcción de un estado más participativo, eficiente y transparente, Movilidad Futura SAS, 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 el 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.

PLANEACIÓN	Código: PInst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

2. OBJETIVO GENERAL

La Política de seguridad digital, busca definir las estrategias, mecanismos y lineamientos mediante los cuales se desarrolla e implementa dicha Política, la cual está comprometida con tres pilares fundamentales de la seguridad de la información - confidencialidad, integridad y disponibilidad, mediante la gestión y control de la implementación de la seguridad digital al interior de la entidad, por medio de la definición de roles y responsabilidades en seguridad, la separación de deberes, el contacto con las autoridades y grupos de interés, la incorporación de la seguridad en la gestión de los proyectos y la definición de controles para la mitigación de riesgos digitales, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones Min TIC.

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.

2.1. OBJETIVOS ESPECIFICOS

- Definir, precisar y formalizar los elementos normativos sobre aspectos de protección de la información.
- Aplicar los lineamientos necesarios en seguridad que permitan proteger los activos de información, buscando mantener la confidencialidad, disponibilidad e integridad de estos, cumpliendo con los requisitos legales vigentes aplicables a la naturaleza de la entidad en materia de seguridad digital.
- Facilitar de manera integral, la gestión de los riesgos de seguridad digital y continuidad de la operación institucional.
- Garantizar la integridad, confidencialidad y el acceso a la información de acuerdo con los niveles y criterios de seguridad establecidos por la entidad y los exigidos por la normatividad vigente.
- Mitigar el impacto de los incidentes de seguridad digital, de forma eficiente, efectiva, eficaz.
- Minimizar y dar tratamiento integral a los riesgos de seguridad digital, para que sean conocidos y gestionados de forma eficiente.

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 eficientemente en el Subproceso de Tecnología, para la entidad Movilidad Futura S.A.S.

Por lo anterior, esta política aplica para toda la entidad, sus funcionarios, contratistas, usuarios internos y externos que acceden o hacen uso de cualquier activo de información, así como exfuncionarios y ex contratistas que hayan tenido acceso a cualquier activo de información, independientemente de su ubicación, medio o formato, así como a la ciudadanía en general que se relacione con el ente de control:

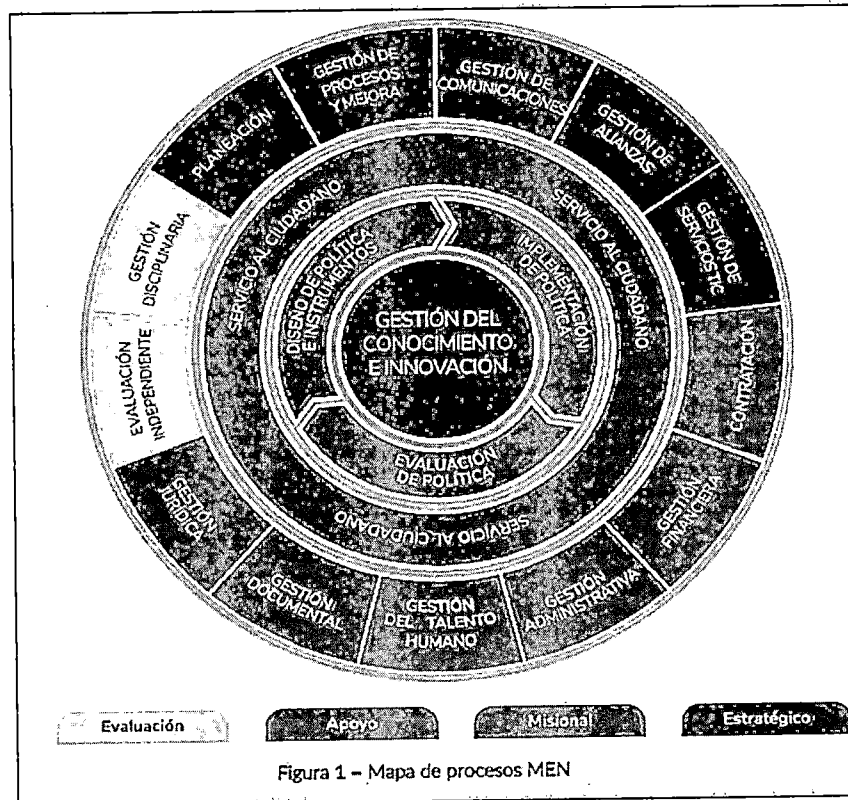


Figura 1 – Mapa de procesos MEN

PLANEACIÓN	Código: Plnst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

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., formalizara y garantizara los tres pilares fundamentales de la seguridad digital tales como:

- La Confidencialidad.
- La Integridad.
- La disponibilidad.

Así mismo gestionando y controlando la implementación de la seguridad digital al interior de la empresa, por medio de la identificación de roles y responsabilidades, la separación de deberes, el contacto con las autoridades, 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 lo anterior alineado con la política de Gobierno Digital y el Modelo de Seguridad Digital, el cual en Movilidad Futura S.A.S., está a cargo del proceso de Gestión Administrativa y este a su vez asignado al subproceso de Tecnología.

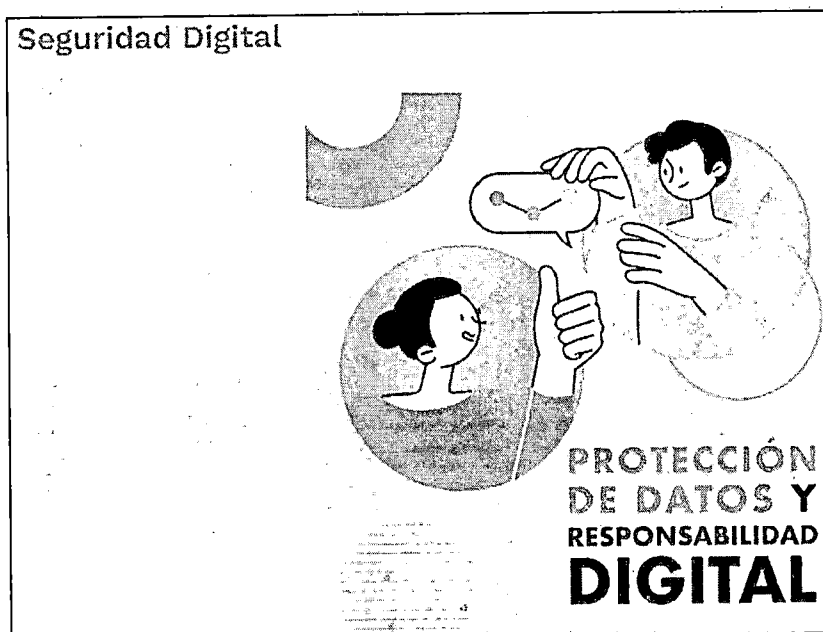
Por lo anterior Movilidad Futura S.A.S., se compromete a implementar y propender por la preservación de la información mediante:

- La comprensión de las necesidades y expectativas de las partes interesadas.
- La determinación del alcance del Modelo de Seguridad y Privacidad de la Información –MSPI.
- La definición, socialización, aplicación y seguimiento de la política de seguridad Digital.
- La definición de roles y responsabilidades en seguridad digital.
- El contacto con las autoridades y grupos de interés.
- La incorporación de la seguridad digital en la gestión de los proyectos.

PLANEACIÓN	Código: Plnst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

- La identificación y clasificación de los activos de información.
- La identificación, valoración y definición del plan de tratamiento de riesgos de seguridad digital.
- La definición de controles para la mitigación de los riesgos, reduciéndolos a un nivel aceptable.

De otro lado, el Modelo Gestión de Riesgos de Seguridad Digital (GRSD) busca brindar un marco para la identificación de las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital e impulsar la prosperidad económica y social de la entidad.





PLANEACIÓN	Código: PInst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025



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 las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 23 de 1982. Derechos de autor.

Ley 527 del 1999. Es una ley que define y regula el uso de mensajes de datos, el comercio electrónico y las firmas digitales. En esencia, esta ley equipara la validez jurídica de los documentos electrónicos y firmas digitales con los documentos físicos y firmas manuscritas, siempre y cuando cumplan con ciertos requisitos.

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

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

Ley 962 de 2005. Simplificación y Racionalización de Tramites y atributos de seguridad en la información electrónica de entidades públicas.

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

Ley 1150 de 2007. Seguridad de la información electrónica en contratación en línea.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas 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

PLANEACIÓN	Código: PInst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan 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.

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.

Ley 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 1755 de 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 de 2016. Política Nacional de Seguridad Digital.

Decreto 2364 de 2012. Firma Electrónica.

Decreto 2609 de 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 de 2015. Por medio del cual se expide el decreto reglamentario del sector de las tecnologías de la información y las comunicaciones.



PLANEACIÓN	Código: Pinst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025



Alcaldía de Popayán

6. DEFINICIONES

Activo de información: Es cualquier elemento, ya sea físico o digital, que contenga o maneje información valiosa para una organización y que, por lo tanto, necesita ser protegido. Estos activos pueden incluir datos, documentos, software, hardware, redes, sistemas y hasta el conocimiento de las personas dentro de la organización.

Amenazas: Se define como cualquier circunstancia o evento con el potencial de causar daño a un sistema o red informática, incluyendo la pérdida, divulgación, modificación o destrucción de datos, o la negación de servicio.

Análisis de Riesgo: Es un proceso sistemático para identificar, evaluar y priorizar amenazas potenciales que podrían afectar la seguridad, la integridad o la disponibilidad de los sistemas y la información.

Alineamientos: Son un conjunto de directrices, políticas, estándares y especificaciones que guían el desarrollo, implementación y uso de tecnologías de la información y la comunicación (TIC).

Arquitectura: Identifica los requerimientos a partir de las necesidades de capacidades y servicios de tecnología que se han definido en la arquitectura institucional, la arquitectura de información, la arquitectura de sistemas de información y la arquitectura de seguridad.

Ataque Cibernético: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (Documento Modelo Nacional Riesgo de Seguridad Digital).

Confidencialidad: Es el Acceso a la información por parte únicamente de quienes estén autorizados. Según ISO IEC13335-1:2004 es la característica/propiedad por la que la información no está disponible o es revelada a individuos, entidades, o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Alcaldía Distrital de Cartagena de Indias. Ejemplo: archivo de Word "listado de personal.docx"

PLANEACIÓN	Código: Plinst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

Estándar: Conjunto de reglas, especificaciones o prácticas acordadas que se utilizan para asegurar la compatibilidad, interoperabilidad y calidad en el desarrollo y uso de productos, procesos y servicios tecnológicos. Los estándares facilitan la comunicación entre diferentes sistemas, garantizan la seguridad y promueven la eficiencia en el ámbito tecnológico.

Entorno Digital: Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

Gestión de Riesgos de Seguridad Digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

Incidente Digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

Seguridad de la Información: "Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua, con miras a preservar la confidencialidad, integridad, y disponibilidad de la información" (ISO/IEC 27000).

Riesgo de Seguridad Digital: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.

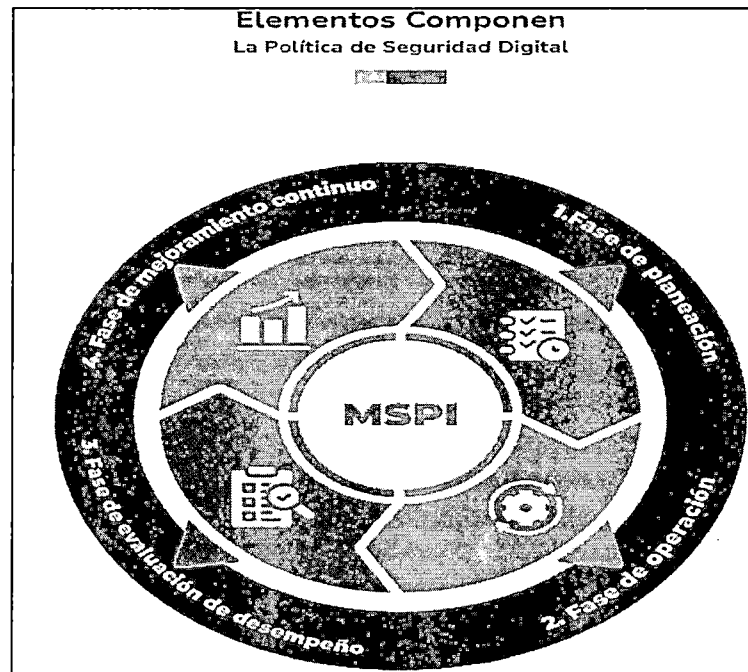
Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (Documento CONPES 3854).

Virus: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

PLANEACIÓN	Código: Plinst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

7. IMPLEMENTACIÓN DE LA POLITICA DE SEGURIDAD DIGITAL

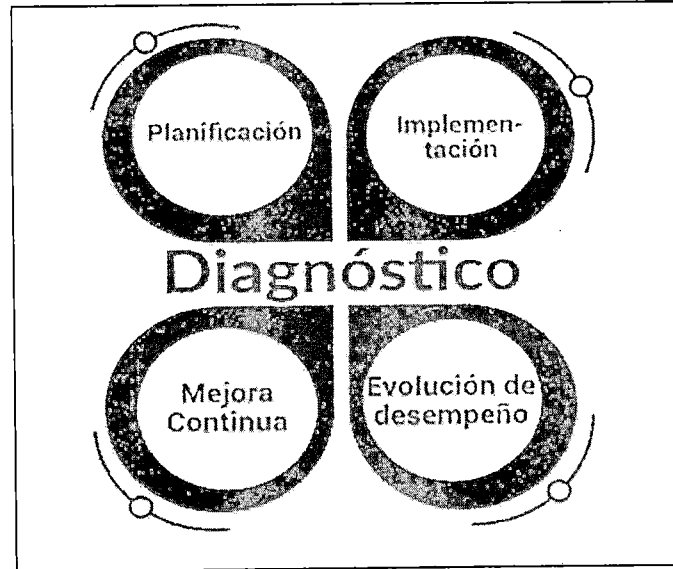
Movilidad futura S.A.S., con el objeto de articular los esfuerzos, recursos, metodologías y estrategias, asegurará la implementación de la política de Seguridad Digital, designando como responsable de la Seguridad digital al Proceso Administrativo, el cual estará destinado a cargo del Subproceso de Tecnología.



(Modelo de Seguridad y Privacidad de la Información –MSPI)

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 Riesgo de Seguridad digital, dispuesto por la Min TIC, se dará cumplimiento a las actividades relacionadas en el plan de acción.

PLANEACIÓN	Código: PInst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025



Para establecer la compatibilidad de la presente política y los objetivos del Modelo de Seguridad digital, la entidad se compromete a:

- Minimizar el riesgo de seguridad digital, seguridad de la información y privacidad de la información de los procesos y activos de información de la Entidad.
- Cumplir con los principios de seguridad digital, dispuestos por la Función Administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros sobre la confidencialidad, integridad y disponibilidad de la información que se genera, administra, custodia, modifica en y para la entidad.
- Apoyar la innovación tecnológica en la Entidad, al igual que proteger los activos de información de la entidad.
- Establecer las políticas, procedimientos, guías e instructivos en materia de Seguridad y Privacidad de los datos e información de la entidad.

PLANEACIÓN	Código: Plnst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

Categoría	Actividades de Gestión	Estrategias o Mecanismos	Área Responsable	Periodicidad
Gestión de servicios TIC	Diseño, definición o actualización de los documentos y controles	Política de Seguridad digital	Administrativa Subproceso de Tecnología Proceso de Planeación	Anual
	Diseño, definición o actualización de la Gestión de levantamiento de activos de información.	Inventario de activos de información		
	Diseño, definición o actualización de la Gestión de los riesgos de seguridad digital.	Riesgo de información.		

PLANEACIÓN	Código: PInst-12-PL-1
POLÍTICA DE SEGURIDAD DIGITAL	Versión: 02
	Fecha: 29/10/2025

8. ACCIONES PARA MANTENER LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

En Movilidad Futura S.A.S., se establecen las siguientes acciones para mantener el estado de implementación de la política de Seguridad Digital de la siguiente manera:

1. Revisión de políticas de Seguridad Digital y mecanismos que permitan verificar su cumplimiento.
2. Revisión y aprobación de los activos y riesgos de Seguridad Digital.
3. Verificar los riesgos de seguridad digital definidos en la matriz de riesgos.
4. Revisión de indicadores asociados a los objetivos con el fin de verificar su cumplimiento y alineación.
5. Contar con un Software actualizado, para la prevención de ataques cibernéticos.
6. Establecer procedimientos, guías e instructivos en materia de Seguridad y Privacidad de los datos e información de la entidad.
7. Mantener la información que se genera, administra, modifica en y para la entidad, de los funcionarios, contratistas y terceros, custodiada y segura.



AMENAZAS Y RIESGOS EN LA SEGURIDAD DIGITAL

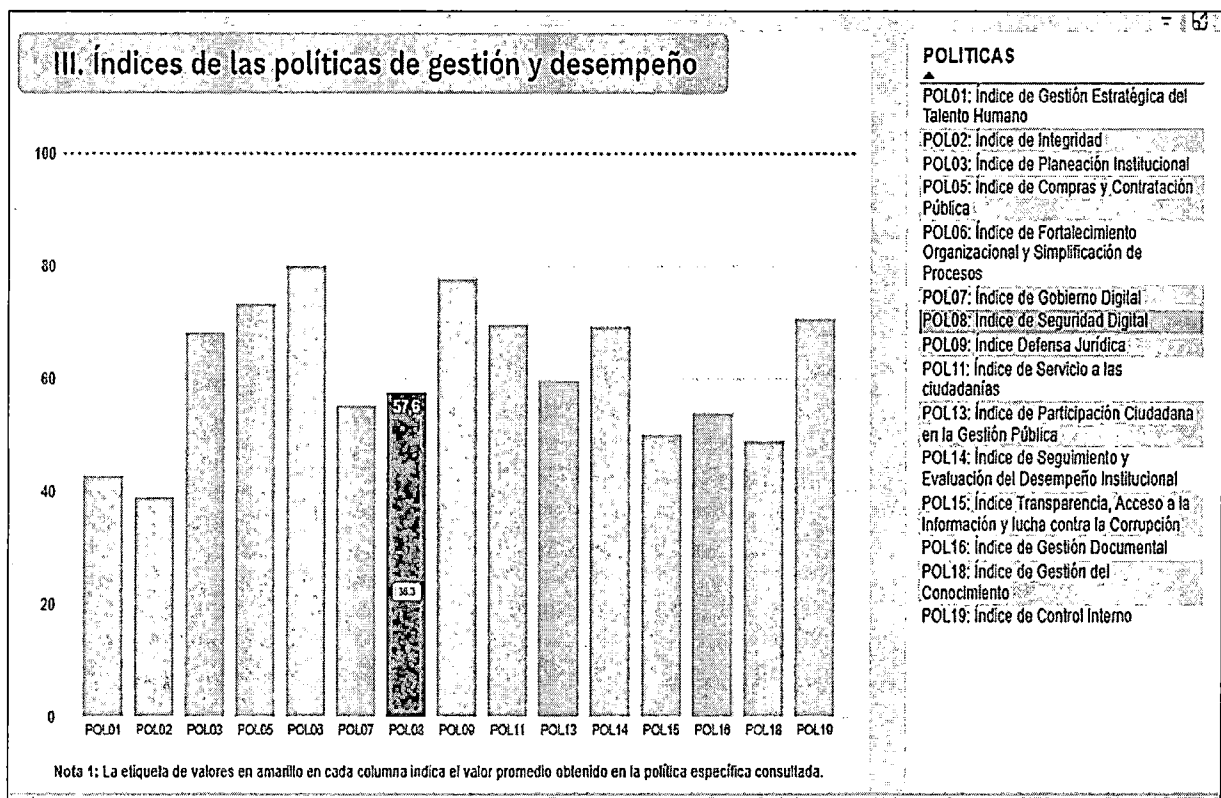
1. Phishing
Busca engañarte para que reveles información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web falsificados.

2. Malware
Programas maliciosos, como virus, troyanos o ransomware. Pueden infectar tu dispositivo y comprometer tus datos personales o incluso bloquear el acceso a tus archivos.

3. Vulnerabilidades en el software
Errores o debilidades en el software pueden ser aprovechados por los ciberdelincuentes para obtener acceso no autorizado a tu información.


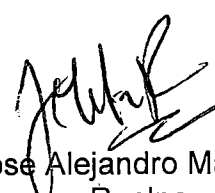
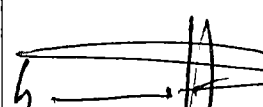
9. RESULTADOS DE MEDICIÓN DE DESEMPEÑO INSTITUCIONAL VIGENCIA 2024 - POLÍTICA DE SEGURIDAD DIGITAL

A continuación, se presentarán los resultados de medición y desempeño institucional, presentados por el Modelo Integrado de Planeación y Gestión MIPG vigencia 2024, de la política de Seguridad Digital.



NOTAS DE CAMBIO

VERSIÓN	FECHA	MOTIVO CAMBIO
02	29/10/2025	<ul style="list-style-type: none"> - Se hizo ajustes a la plantilla del documento, debido a que se actualizo de la versión, fecha y dirección de la entidad. - Se incluyeron objetivos específicos. - Se actualizo la descripción de la política. - Se actualizo el Marco de Referencia. - Se actualizaron las definiciones. - Se actualizo la implementación de la política. - Se incluyó acciones para mantener la implementación de la política. - Se incluyó los resultados de medición de desempeño institucional MIPG - vigencia 2024.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma:  Jackeline Sotelo Cerón	Firma:  Jose Alejandro Martínez Realpe	Firma:  Gerardo Cruz Jiménez
Contratista Apoyo Planeación	Contratista Coordinador de la Gestión del Proceso de Planeación	Gerente (E)

Proyectó: Jackeline Sotelo Cerón – Contratista Apoyo de Planeación
 Revisó: Juan Manuel Muñoz - Contratista Apoyo Gestión Administrativa
 Revisó: Diana Zugeidy Urbano Silva – Contratista Coordinador de la Gestión del Proceso de Administrativa