POLÍTICA GENERAL
DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El IMRDS con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de El IMRDS, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a el IMRDS
b) **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con El IMRDS, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
b) **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
c) **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
d) **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
e) **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

OBJETIVOS

a) Preservar, proteger y administrar de forma eficiente la información de El IMRDS junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información de El IMRDS, para asegurar la sostenibilidad de El IMRDS y el nivel de eficacia.

ALCANCE

Esta política es de aplicación en el conjunto de Direcciones, oficinas y dependencias que componen El IMRDS, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal del IMRDS, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

NIVEL DE CUMPLIMIENTO

- ✓ El IMRDS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen los 12 principios de seguridad que soportan el MSPI de El IMRDS:

1. El IMRDS ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del Instituto, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de funcionarios provisionales, funcionarios con carrera administrativa, funcionarios con libre nombramiento y contratistas.
3. El IMRDS, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, incluyendo los datos personales conforme lo define la Ley 1581 de 2012 y las normas que complementen, definen o reglamentan.
4. El IMRDS, protegerá la información creada, procesada, transmitida o resguardada por sus procesos del instituto, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. El IMRDS, protegerá su información de las amenazas originadas por parte del personal.
6. El IMRDS, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. El IMRDS, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. El IMRDS, implementará control de acceso a la información, sistemas y recursos de red. POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
9. El IMRDS, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. El IMRDS, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. El IMRDS, garantizará la disponibilidad de sus procesos del instituto y la continuidad de su operación basada en el impacto que pueden generar los eventos.
12. El IMRDS, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA DE APROBACIÓN DD/MM/AA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**
01	27/10/2021	Creación Política de Seguridad y Privacidad de la Información	Líder Oficina TIC

TABLA DE APROBACIÓN		
ELABORÓ	**REVISIÓN**	**APROBÓ**
Nombre: Edwin Zapata **Cargo:** Líder de Sistemas **Firma:** *Original Firmado* **Fecha:** 27 octubre de 2021	**Nombre:** Karen Mora Cruz **Cargo:** Líder MIPG **Firma:** *Original Firmado* **Fecha:** 27 octubre de 2021	**Nombre:** Comité Institucional de Gestión y Desempeño. **Acta No.**07 de 2021 **Fecha:** 27 octubre de 2021