POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO GENERAL

Establecer el marco estratégico para planear, implementar, evaluar y mejorar de manera continua el SGSI, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información en todos los procesos del IDEA.

1.1. OBJETIVOS ESPECIFICOS:

- ✓ Fortalecer la cultura institucional en seguridad de la información mediante programas continuos de sensibilización y capacitación, orientados a incrementar la conciencia, apropiación y adopción de prácticas seguras por parte de servidores, contratistas y terceros frente a los riesgos, amenazas y responsabilidades asociadas al manejo de la información.
- ✓ Consolidar progresivamente la madurez operativa del modelo de seguridad basado en el principio de cero confianza, mediante la implementación y evaluación continua de controles sobre identidades, dispositivos, aplicaciones, red y datos, con el fin de reducir la exposición a accesos no autorizados y a amenazas internas y externas.
- ✓ Optimizar los procesos de detección, análisis, respuesta y recuperación de incidentes de seguridad de la información, ciberseguridad y protección de datos personales, incorporando mecanismos de revisión, lecciones aprendidas y mejora continua en todas sus etapas, con el fin de reducir los tiempos de respuesta y minimizar los impactos operativos, financieros y reputacionales, en alineación con buenas prácticas y estándares.
- ✓ Incrementar la madurez del Sistema de Gestión de Seguridad de la Información (SGSI) mediante la evaluación periódica de su desempeño y la implementación de acciones de mejora continua, con el fin de fortalecer la gestión de la seguridad de la información y la resiliencia institucional.
- ✓ Identificar, analizar, evaluar y tratar de manera sistemática los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información, aplicando el ciclo PHVA para asegurar la mejora continua del SGSI, la eficacia de los controles y su alineación con estándares internacionales y regulaciones nacionales.
- ✓ Establecer lineamientos para la protección, confidencialidad, integridad y uso adecuado de los datos personales tratados por la organización, conforme a la Ley 1581 de 2012 y demás normas aplicables.

2. ALCANCE Y APLICABILIDAD

La presente política cubre todos los activos de información, sistemas y procesos del Instituto, en entornos físicos, digitales y en la nube, sin importar que no se encuentre incluido explícitamente en este documento.

Esta política es de obligatorio cumplimiento para todos los servidores, contratistas, practicantes, proveedores y terceros, y todas aquellas personas naturales o jurídicas que tengan acceso a los activos de la información del IDEA.

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La presente política se fundamenta en buenas prácticas y estándares internacionales de seguridad de la información y ciberseguridad, especialmente en la norma ISO/IEC 27001:2022 y su enfoque de mejora continua. Asimismo, se desarrolla en cumplimiento de la normativa nacional aplicable, incluyendo la Ley 1581 de 2012 de protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, la Ley 1273 de 2009 sobre delitos informáticos, y demás disposiciones regulatorias relacionadas con seguridad digital, privacidad de la información y gestión del riesgo.

El IDEA reconoce la información como un activo crítico y se compromete a proteger su confidencialidad, integridad, disponibilidad y privacidad mediante controles técnicos, humanos, físicos y organizacionales. Esta política se basa en el principio del mínimo privilegio garantizando que los usuarios únicamente dispongan de los permisos estrictamente necesarios para el desempeño de sus funciones.

La ciberseguridad, la privacidad de la información y la continuidad de la operación se adoptan como ejes transversales para mitigar los riesgos y fortalecer la resiliencia institucional. El Instituto promoverá el uso seguro y responsable de los recursos tecnológicos, incluyendo el acceso a internet, dispositivos externos, plataformas digitales y herramientas de inteligencia artificial, mediante controles orientados a prevenir incidentes de seguridad, fuga de información y afectaciones a la operación.

El SGSI se mantendrá bajo un esquema de mejora continua, incorporando la gestión de riesgos, incluyendo los derivados del cambio climático, que puedan afectar la infraestructura tecnológica y la disponibilidad de los servicios. La política se desarrolla en concordancia con la misión y visión del IDEA, dando el cumplimiento a los requisitos legales y regulatorios aplicables, y atendiendo las expectativas de las partes interesadas internas y externas.

La relación con los proveedores y terceros se gestionará bajo criterios de seguridad de la información, velando por el cumplimiento de los lineamientos establecidos y que se alineen con la protección de los activos institucionales.

La gestión de incidentes será un componente esencial, para garantizar la detección temprana, el análisis, la respuesta y la recuperación efectiva.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección respalda y lidera la Política de Seguridad de la Información, asegurando la disponibilidad de los recursos necesarios e integrando la seguridad, la ciberseguridad, la privacidad de la información y la continuidad de la operación en la estrategia y cultura institucional. Asimismo, realiza seguimiento al desempeño del SGSI y promueve la mejora continua para asegurar su efectividad y alineación con los objetivos del Instituto.

5. ROLES Y RESPONSABILIDADES

Junta Directiva
Aprueba la Política General de la Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información del Instituto.

Alta Dirección – Gerencia General
Respaldar el cumplimiento de la Política General de la Seguridad de la Información a nivel organizacional, fomentando una cultura de compromiso y asegurando la disponibilidad de los recursos necesarios para su adecuada implementación, operación y mejora continua.

Gerencia de Riesgo y Dirección de Ciberseguridad y Seguridad de la Información
Liderar, coordinar y promover la implementación y cumplimiento de la Política General de Seguridad de la Información en el Instituto, articulando su aplicación en los diferentes procesos institucionales. Asimismo, realizar el seguimiento, medición y evaluación del desempeño del SGSI, identificando brechas, oportunidades de mejora y acciones orientadas al fortalecimiento continuo de la seguridad de la información.

Auditoría Interna.
Evaluar de manera independiente y objetiva la efectividad y el cumplimiento del SGSI y de la Política General de Seguridad de la Información, verificando la adecuada aplicación de controles y emitiendo recomendaciones orientadas al fortalecimiento y mejora continua del sistema.

Control Interno Disciplinario
Adelantar las actuaciones disciplinarias relacionadas con el incumplimiento de la Política General de Seguridad de la Información, contribuyendo a su observancia mediante la aplicación de las medidas correctivas correspondientes, conforme al marco normativo vigente.

Oficina de TI
Asegurar la implementación y aplicación de los lineamientos de la Política General de Seguridad de la Información en la infraestructura tecnológica y los sistemas de la entidad, contribuyendo al fortalecimiento de la seguridad digital y apoyando la gestión de los riesgos e incidentes asociados a los servicios tecnológicos.

Dirección de Talento Humano
Promover la aplicación de la Política General de Seguridad de la Información en la gestión del personal, contribuyendo al fortalecimiento de la cultura organizacional, al cumplimiento de los lineamientos establecidos y a la adopción de buenas prácticas por parte de los servidores.

Directores y jefes de Oficina
Promover y asegurar la aplicación de la Política General de Seguridad de la Información en los procesos bajo su responsabilidad, contribuyendo al cumplimiento de los lineamientos establecidos, a la protección de los activos de información que gestiona su dependencia y al fortalecimiento de la cultura de seguridad de la información en la entidad.

Oficial de Datos Personales
Coordinar la definición, implementación, seguimiento y mejora del Programa Integral de Gestión de Datos Personales del Instituto, asegurando el cumplimiento de la normativa aplicable en materia de protección de datos personales. Asimismo, deberá promover la adopción de controles administrativos, técnicos y organizacionales orientados a garantizar la confidencialidad, integridad, disponibilidad y uso adecuado de la información personal, así como apoyar la gestión de incidentes, requerimientos de titulares y acciones de sensibilización institucional en esta materia.

Funcionarios, contratistas, terceros
Cumplir la Política General de Seguridad de la Información, haciendo un uso adecuado de los activos de información, aplicando los lineamientos establecidos y reportando

oportunamente cualquier evento o situación que pueda afectar la seguridad de la información de la entidad.

6. GESTIÓN Y DERECHOS DE PROPIEDAD INTELECTUAL

El Instituto reconoce la importancia de proteger los derechos de propiedad intelectual asociados a la información, por ello el Instituto promoverá el respeto y la protección de los derechos de propiedad intelectual asociados a la información, el software y demás activos institucionales, asegurando su uso legal y autorizado.

Se prohíbe el uso, reproducción o distribución no autorizada de estos activos, y se deberá asegurar que todo software y contenido digital cuente con las licencias correspondientes. Para su protección, la entidad implementará controles de acceso, clasificación de la información y medidas que prevengan su pérdida o uso indebido.

7. APROBACIÓN Y REVISIONES A LA POLÍTICA

La presente Política General de Seguridad de la Información será aprobada por la Junta Directiva del Instituto y tendrá carácter obligatorio para todos los funcionarios, contratistas y terceros que accedan a la información institucional.

Su revisión se realizará de manera anual, o cuando se presenten cambios significativos en el contexto institucional, normativo, tecnológico o de riesgos, con el fin de mantener su pertinencia, alineación estratégica y efectividad en la protección de la información.

8. USO Y SUPERVISIÓN

IDEA se reserva el derecho de monitorear, revisar, auditar y acceder a la información almacenada, procesada o transmitida a través de los recursos, herramientas, plataformas, cuentas y dispositivos institucionales, incluyendo, pero sin limitarse a, correo electrónico corporativo, equipos de cómputo, sistemas de información, servicios de almacenamiento, redes de telecomunicaciones y herramientas de colaboración.

Las actividades de monitoreo, seguimiento, revisión y auditoría podrán ser realizadas por las dependencias competentes, de acuerdo con sus funciones y responsabilidades institucionales.

En particular, la Gerencia de Riesgos, en el marco de las funciones relacionadas con seguridad de la información y ciberseguridad, podrá efectuar actividades de monitoreo técnico, análisis, correlación de eventos, revisión de registros (logs), detección de

incidentes, vulnerabilidades, amenazas, verificación de controles, evaluación de exposición al riesgo y demás actividades orientadas a la protección de los activos de información, la infraestructura tecnológica y la gestión de riesgos de seguridad digital.

Así mismo, la Oficina de Control Interno Disciplinario podrá acceder a la información y evidencias digitales cuando se requiera para el adelantamiento de actuaciones disciplinarias, investigaciones internas o atención de requerimientos efectuados por autoridades competentes, entes de control o autoridades judiciales, en el marco de sus funciones legales. Todas las actividades de supervisión y monitoreo deberán realizarse en cumplimiento de la normatividad vigente, los principios de necesidad, proporcionalidad, confidencialidad y debido proceso, garantizando la protección de los datos personales y la reserva de la información a que haya lugar.

9. EXCEPCIONES

Las excepciones a la presente Política requerirán la aprobación del Comité de Riesgos y se concederán exclusivamente para el desarrollo de funciones del empleo público.

La Gerencia de Riesgos revisará la viabilidad de dar permisos temporales con el fin de no afectar la continuidad del negocio previo análisis del riesgo.

Los incumplimientos y exclusiones deberán documentarse por parte de la Dirección de Ciberseguridad y Seguridad de la Información.

10. SANCIONES

El incumplimiento de la Política General de Seguridad de la Información dará lugar a una investigación para la aplicación de las medidas disciplinarias, administrativas, civiles o penales a que haya lugar, de conformidad con la normatividad vigente.

11. DEFINICIONES

Confidencialidad: Asegura que la información solo sea accesible para personas autorizadas. Su propósito es evitar el acceso indebido y proteger los datos frente a divulgaciones no autorizadas.

Continuidad de la Operación: Capacidad de la entidad para mantener la prestación de sus servicios críticos ante situaciones de contingencia o desastres, mediante planes de recuperación y resiliencia.

Integridad: Garantiza que los datos sean precisos, completos y confiables. Se busca preservar la exactitud de la información y evitar alteraciones no autorizadas.

Disponibilidad: Permite que la información esté accesible cuando se requiera por usuarios autorizados. Esto asegura que los procesos institucionales no se vean interrumpidos por falta de acceso a los datos**.**

Gestión de Incidentes: Comprende las acciones de detección, análisis, respuesta y recuperación frente a eventos que afectan la seguridad. Es un proceso clave para reducir impactos y fortalecer la resiliencia institucional.

Inteligencia Artificial: Disciplina de la informática que crea sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como aprender, razonar, reconocer patrones o tomar decisiones.

SGSI: El Sistema de Gestión de Seguridad de la Información (SGSI) es el conjunto de políticas, procesos, procedimientos, recursos y controles mediante los cuales una entidad gestiona de manera sistemática la seguridad de la información, con el propósito de proteger su confidencialidad, integridad, disponibilidad y privacidad, mediante la identificación, evaluación y tratamiento de los riesgos, y asegurando el cumplimiento de la normatividad vigente y la mejora continua.

ZERO TRUST (Confianza Cero): Es un enfoque de seguridad en el que ningún usuario, dispositivo o sistema se considera confiable por defecto, por lo que todo acceso a la información debe ser verificado y autorizado de manera continua, aplicando el principio de mínimo privilegio.

PHVA: Es un ciclo de mejora continua que permite planificar, implementar, evaluar y ajustar las acciones orientadas a la protección y gestión de la seguridad de la información.

CONTROL DE VERSIONES			
Versión	Fecha	Descripción	Responsable
1.0	Octubre/2017	Versión inicial del documento	Oficina de Tecnologías de la Información
2.0	Diciembre/2018	Adopción de las Políticas al Sistema de Gestión de Seguridad de la Información de las MINTIC y adición de Políticas de Ciberseguridad.	Oficina de Tecnologías de la Información
3.0	Febrero/2023	Actualización de las nuevas herramientas implementadas y procedimientos.	Dirección de Ciberseguridad y Seguridad de la Información
4.0	Mayo/2026	Actualización a la Norma ISO 27001:2022	Dirección de Ciberseguridad y Seguridad de la Información