



**POLÍTICA GENERAL DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN**

Código: GT-SP-MA-01
Fecha Vigencia: 17/04/2023
Versión: 1

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN


**INSTITUTO DE VALORIZACIÓN DE MANIZALES
- INVAMA -**

2023



TABLA DE CONTENIDO

1. OBJETIVO	2
2. DEFINICIONES/GLOSARIO	2
3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	2
4. COMPROMISO DE LA ALTA DIRECCIÓN	3
5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	4
6. APLICABILIDAD.....	4
7. CUMPLIMIENTO.....	4
8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES).....	5
9. SANCIONES	8
10. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI.....	8
11. APROBACIÓN Y REVISIONES A LA POLÍTICA	9

	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GT-SP-MA-01 Fecha Vigencia: 1704/2023 Versión: 1
---	---	---

1. OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección del **INSTITUTO DE VALORIZACIÓN DE MANIZALES – INVAMA** -, para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.


2. DEFINICIONES/GLOSARIO

- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

3. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El **INSTITUTO DE VALORIZACIÓN DE MANIZALES – INVAMA**, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Para el **INVAMA**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad,

	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: GT-SP-MA-01 Fecha Vigencia: 1704/2023 Versión: 1
---	---	---


confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, contratistas, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del MSPI estarán determinadas por las siguientes premisas:

- Gestionar de manera eficaz los riesgos de seguridad y privacidad de la información identificada en la entidad.
- Cumplir con los niveles requeridos de confidencialidad, integridad y disponibilidad establecidos por la entidad.
- Cumplir con los criterios y requisitos de seguridad atendiendo el marco normativo y legal de la entidad.
- Mantener la confianza digital en las partes interesadas internas y externas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer y sensibilizar la cultura de Seguridad de la Información en los funcionarios, contratistas, terceros, aprendices, practicantes y usuarios del INVAMA.
- Garantizar la continuidad del negocio frente a incidentes.
- INVAMA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de **INVAMA** se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información (MSPI); así mismo, se compromete a revisar el avance de la implementación del MSPI de manera periódica y también garantizará los recursos suficientes

	<p>POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Código: GT-SP-MA-01 Fecha Vigencia: 1704/2023 Versión: 1</p>
---	---	---

(tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la Entidad.

6. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la Entidad, servidores públicos, contratistas, aprendices, practicantes, terceros y partes interesadas de la Entidad, que en el ejercicio de sus funciones utilicen información y servicios de tecnología de la información del **INVAMA**.

7. CUMPLIMIENTO

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por todos los actores definidos en el alcance/aplicabilidad establecidos en el presente documento.

- **INVAMA** protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos de información que hacen parte de los mismos.
- **INVAMA** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, 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.
- **INVAMA** protegerá su información de las amenazas originadas por parte de los usuarios internos y externos.
- **INVAMA** protegerá la infraestructura tecnológica que soporta sus procesos críticos.
- **INVAMA** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.



- **INVAMA** implementará control de acceso a la información, sistemas y recursos de red.
- **INVAMA** garantizará que la seguridad y privacidad de la información sea parte integral del ciclo de vida de los sistemas de información.
- **INVAMA** garantizará a través de una adecuada gestión de los eventos de seguridad y privacidad de la información y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad y privacidad.
- **INVAMA** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los incidentes que afecten la seguridad y privacidad de la información.
- **INVAMA** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de seguridad y privacidad de la información.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, 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.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

INVAMA, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos, entre otros):


ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Alta Dirección	<ul style="list-style-type: none">• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).• Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.



ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Tecnologías de Información	<ul style="list-style-type: none">• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.• Participar en la elaboración del cronograma de capacitación de seguridad digital en la Entidad.
Responsable de Seguridad Digital, Seguridad de la Información y Protección de Datos Personales	<ul style="list-style-type: none">• Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad.• Establecer lineamientos para la protección de los datos personales tratados en la Entidad.• Diseñar y presentar para aprobación lineamientos (políticas, manuales, procedimientos y formatos) que fortalezcan la seguridad de la información y permitan el establecimiento y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información en la Entidad.
Gestión Humana	<ul style="list-style-type: none">• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.



ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Control Interno	<ul style="list-style-type: none">• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.• Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Prensa / Comunicación Interna	<ul style="list-style-type: none">• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.
Oficina Jurídica y Contratación	<ul style="list-style-type: none">• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad.• Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Líderes de Proceso	<ul style="list-style-type: none">• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).• Identificar, informar e inventariar los nuevos activos de información y los riesgos cibernéticos asociados.
Partes Interesadas (Funcionarios, contratistas, Proveedores)	<ul style="list-style-type: none">• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos.• Cumplir a cabalidad con las políticas y procedimientos de seguridad y privacidad de la información definida y aprobada.

	<p align="center">POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Código: GT-SP-MA-01 Fecha Vigencia: 1704/2023 Versión: 1</p>
---	---	--

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
<p align="center">Comité Institucional de Gestión y Desempeño</p>	<ul style="list-style-type: none"> • Comunicar a los funcionarios, contratistas y/o particulares que participan de forma o indirecta con la Entidad, la importancia de satisfacer los requisitos de seguridad digital.

9. SANCIONES


a. Cualquier violación a las políticas de seguridad de la información de **INVAMA** debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

b. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

10. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

INVAMA indica que realizará revisiones periódicas al MSPI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

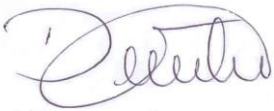
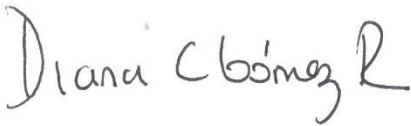

- Revisión de indicadores definidos para el Modelo de Seguridad y Privacidad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.


	<p align="center">POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Código: GT-SP-MA-01 Fecha Vigencia: 1704/2023 Versión: 1</p>
---	---	--

11. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Alta Dirección o el Comité de Gestión y Desempeño. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (reestructuración de áreas o procesos) o en su infraestructura tecnológica.
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.
4. Control de cambios en los sistemas de información que se encuentren en producción.
5. Cambios en los procesos, en los objetivos del sistema o de la organización.
6. Cambios normativos que en materia de seguridad de la información emita el gobierno nacional a través del Ministerio de las Tecnologías de la Información y Comunicaciones – MinTIC o del Departamento Administrativo de la Función Pública entre otros.

ELABORÓ	REVISÓ	APROBÓ
 <p>Nombre: DIANA LORENA CORTÉS JIMÉNEZ Cargo: TÉCNICO ADMINISTRATIVO SISTEMAS Fecha: 12-04-2023</p>	 <p>Nombre: DIANA CONSTANZA GÓMEZ RAMÍREZ Cargo: PROFESIONAL UNIVERSITARIO SISTEMAS Fecha: 14-04-2023</p>	 <p>Nombre: MAURICIO CÁRDENAS RAMÍREZ Cargo: GERENTE Fecha: 17-04-2023</p>

	<p align="center">POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	<p>Código: GT-SP-MA-01 Fecha Vigencia: 1704/2023 Versión: 1</p>
---	---	--

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
17-04-2023	1	Creación Política General de Seguridad y Privacidad de la Información