INSTITUTO DE VALORIZACIÓN DE MANIZALES
INVAMA

POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Entidad:	Instituto de Valorización de Manizales — INVAMA
Versión:	2.0
Fecha de elaboración:	06-05-2026
Fecha de aprobación:	Acta 005 del 26-05-2026
Elaborado por:	Diana Lorena Cortés Jiménez Técnico Administrativo Sistemas
Revisado por:	Luz Adriana Blandón Correa Profesional Universitario Sistemas
Aprobado por:	Comité de Gestión y Desempeño Institucional

1- INTRODUCCIÓN

El instituto de valorización como entidad pública descentralizada de la alcaldía del municipio de Manizales encargada de la administración del alumbrado público, el alumbrado navideño y las obras por valorización de la ciudad presenta a través del presente documento la política institucional de **SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** con la cual busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información, mitigando riesgos de seguridad, asegurando el cumplimiento legal/normativo y protegiendo los datos personales contra accesos no autorizados.

La presente política responde a los lineamientos de la dimensión No. 03 Gestión con Valores para Resultados del modelo integrado de planeación y gestión adoptado por la entidad mediante resolución 006 de 10 de enero de 2026.

2- MARCO LEGAL Y DERECHOS QUE GARANTIZA

La presente política se fundamenta en el siguiente marco normativo vigente:

Norma	Relevancia para INVAMA
Ley 1581 de 2012	Régimen de protección de datos personales. INVAMA actúa como Responsable del Tratamiento.
Decreto 1074 de 2015	Compila las disposiciones sobre tratamiento de datos personales (antes Decreto 1377/2013). Regula el RNBD ante la SIC.
Decreto 1078 de 2015	Decreto Único Reglamentario TIC. Base del MSPI para entidades públicas colombianas.
Ley 1712 de 2014	Transparencia y acceso a la información pública. Define información pública, clasificada y reservada.
Ley 527 de 1999	Comercio electrónico, mensajes de datos y firma digital. Sustento del uso de firma electrónica en INVAMA.
Ley 1273 de 2009	Delitos informáticos en Colombia. Tipifica conductas que atentan contra sistemas de información de INVAMA.
Ley 1952 de 2019 mod. por Ley 2094 de 2021	Código General Disciplinario vigente desde el 1 de julio de 2022. Fundamento de sanciones a servidores públicos por incumplimiento de políticas de seguridad.

Norma	Relevancia para INVAMA
Resolución MinTIC 500 de 2021	Lineamientos de seguridad digital para entidades del Estado en el marco de Gobierno Digital.
Resolución MinTIC 02277 de 2025	Marco vigente del MSPI basado en ISO/IEC 27001:2022. Reemplaza la Resolución 000001 de 2016. Referencia obligatoria para el SGSI de INVAMA.
Estrategia Nacional de Ciberseguridad 2024-2028	Política vigente del Estado colombiano en ciberseguridad. Absorbe las líneas de acción del CONPES 3995 de 2020.
ISO/IEC 27001:2022	Estándar internacional para el SGSI. Marco de referencia para establecimiento, implementación y mejora continua.
ISO/IEC 27002:2022	93 controles de seguridad en 4 temáticas. Guía práctica para la implementación de controles en INVAMA.
Ley 594 de 2000	Ley General de Archivos. Regula la gestión documental y retención de información institucional.
Ley 1221 de 2008	Teletrabajo. Marco legal para la modalidad de trabajo remoto de servidores de INVAMA.

3. DEFINICIONES Y GLOSARIO

Para efectos de la presente política, los siguientes términos se entienden conforme a las definiciones de la norma ISO/IEC 27000, la Ley 1581 de 2012 y los lineamientos del MSPI:

Término	Definición
Activo de información	Cualquier información o elemento con valor para INVAMA que debe ser protegido: datos, software, hardware, servicios, personas y procesos.
Amenaza	Causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
Autenticación	Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
Confidencialidad	Propiedad que garantiza que la información es accesible solo para personas, entidades o procesos autorizados.

Término	Definición
Cifrado	Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
Criptografía	Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.
Control de seguridad	Medida técnica, administrativa u operativa implementada para reducir o mitigar un riesgo de seguridad de la información.
Disponibilidad	Propiedad que garantiza que la información y los sistemas son accesibles y utilizables cuando los usuarios autorizados los requieren.
Dato personal	Conforme a la Ley 1581/2012: cualquier información vinculada o que pueda asociarse a personas naturales determinadas o determinables.
Integridad	Propiedad que garantiza la exactitud y completitud de la información, protegiéndola de modificaciones no autorizadas.
Incidente de seguridad	Evento o serie de eventos que comprometen o amenazan la confidencialidad, integridad o disponibilidad de la información de INVAMA.
MSPI	Modelo de Seguridad y Privacidad de la Información del MinTIC: marco de referencia para el SGSI de entidades públicas colombianas.
Riesgo de seguridad	Posibilidad de que una amenaza explote una vulnerabilidad y cause impacto sobre la confidencialidad, integridad o disponibilidad de la información.
SGSI	Sistema de Gestión de Seguridad de la Información: conjunto de políticas, controles, procesos y sistemas implementados por INVAMA para gestionar y proteger su información.
Responsable del Tratamiento	Persona natural o jurídica que decide sobre la base de datos y el tratamiento de datos personales. INVAMA es Responsable del Tratamiento.
Titular del dato	Persona natural cuyos datos personales son objeto de tratamiento por parte de INVAMA.

4- POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto de Valorización de Manizales — INVAMA, entendiendo la importancia estratégica de sus activos de información para el cumplimiento de su misión institucional y la prestación de un servicio eficiente y confiable a los ciudadanos de Manizales, adopta la presente Política General de Seguridad y Privacidad de la Información como la declaración de más alto nivel de su compromiso con la protección de la información.

INVAMA se compromete con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, los estándares ISO/IEC 27001:2022 e ISO/IEC 27002:2022, y la Resolución MinTIC 02277 de 2025, buscando proteger la *confidencialidad, integridad y disponibilidad de los activos de información institucionales y* garantizar la privacidad de los datos personales de los ciudadanos y servidores que confían en la entidad.

Los principios sobre los que se fundamenta el SGSI de INVAMA son:

- Gestionar de manera eficaz y sistemática los riesgos de seguridad y privacidad de la información, adoptando controles proporcionales al nivel de riesgo identificado.
- Garantizar los niveles requeridos de confidencialidad, integridad y disponibilidad de la información institucional, establecidos conforme a su clasificación y criticidad.
- Cumplir con los requisitos legales, normativos y contractuales en materia de seguridad de la información y protección de datos personales, incluyendo la Resolución MinTIC 02277 de 2025 y la Ley 1581 de 2012.
- Mantener la confianza digital con los ciudadanos, entidades del Estado, proveedores, contratistas y demás partes interesadas de INVAMA.
- Proteger los activos de información y la infraestructura tecnológica que soportan los procesos críticos de la entidad.
- Garantizar la continuidad de los procesos misionales de INVAMA ante interrupciones, desastres o incidentes de seguridad graves.
- Fortalecer la cultura de seguridad de la información mediante capacitación y sensibilización permanente de todos los servidores públicos, contratistas y terceros.
- Alinearse con la Estrategia Nacional de Ciberseguridad 2024-2028 del Estado colombiano, adoptando sus lineamientos para la gestión del riesgo digital.
- Implementar, operar y mejorar de forma continua el SGSI institucional, aplicando el ciclo de mejora continua PHVA (Planear-Hacer-Verificar-Actuar).
- Garantizar que la seguridad y privacidad de la información sean parte integral del ciclo de vida de los sistemas de información y de los procesos de adquisición, desarrollo y mantenimiento tecnológico de INVAMA.

5- OBJETIVO

Establecer los lineamientos estratégicos definidos por la Alta Dirección del Instituto de Valorización de Manizales — INVAMA para la gestión de la seguridad y privacidad de la información institucional, en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones, los estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27002:2022, la Estrategia Nacional de Ciberseguridad 2024-2028 y los demás requisitos normativos aplicables a las entidades del sector público colombiano.

5.1 Objetivos específicos

- **Proteger los activos de información.** Identificar, clasificar y proteger los activos de información de INVAMA frente a amenazas internas y externas, garantizando la confidencialidad, integridad y disponibilidad de la información institucional durante todo su ciclo de vida.
- **Gestionar los riesgos de seguridad.** Implementar una metodología sistemática y continua de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, conforme a los lineamientos de la Resolución MinTIC 02277 de 2025 y la guía del DAFP.
- **Garantizar la protección de datos personales.** Asegurar el tratamiento de los datos personales de ciudadanos, servidores públicos y contratistas conforme a los principios establecidos en la Ley 1581 de 2012, en calidad de Responsable del Tratamiento, protegiendo los derechos de los titulares y cumpliendo las obligaciones ante la Superintendencia de Industria y Comercio (SIC).
- **Fortalecer la cultura de seguridad institucional.** Desarrollar competencias, conciencia y comportamientos seguros en todos los servidores públicos, contratistas y partes interesadas de INVAMA, mediante programas periódicos de capacitación y sensibilización en seguridad de la información y privacidad de datos.
- **Cumplir el marco normativo y regulatorio.** Garantizar el cumplimiento de las obligaciones legales, normativas y contractuales en materia de seguridad de la información aplicables a INVAMA como entidad pública, incluyendo el reporte oportuno al FURAG en el componente de seguridad digital del MIPG.
- **Gestionar eficazmente los incidentes de seguridad.** Detectar, responder y recuperarse oportunamente ante incidentes de seguridad de la información, minimizando su impacto sobre la operación institucional y garantizando la notificación a las autoridades competentes en los plazos establecidos por la normativa vigente.
- **Garantizar la continuidad de la operación institucional**. Asegurar la disponibilidad de los procesos misionales y servicios críticos de INVAMA ante interrupciones o desastres, mediante planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) probados periódicamente.
- **Controlar el acceso a la información y los sistemas.** Implementar controles de acceso lógico y físico basados en los principios de mínimo privilegio, necesidad de conocer y separación de funciones, garantizando que solo las personas autorizadas accedan a la información y recursos tecnológicos institucionales.

- **Asegurar las relaciones con proveedores y terceros.** Gestionar los riesgos de seguridad de la información derivados de la relación con proveedores, contratistas y terceros, garantizando que cumplan los estándares de seguridad de INVAMA durante toda la vigencia de su relación contractual.
- **Mejorar continuamente el SGSI.** Evaluar periódicamente la efectividad del Sistema de Gestión de Seguridad de la Información de INVAMA mediante auditorías, indicadores de desempeño y revisiones por la dirección, adoptando acciones de mejora que incrementen progresivamente el nivel de madurez del SGSI institucional.

6- COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de INVAMA, representada por su Gerente General, demuestra su liderazgo y compromiso con el SGSI mediante las siguientes acciones concretas:

- Aprobar la presente Política General de Seguridad y Privacidad de la Información y garantizar su comunicación a todos los servidores públicos, contratistas y partes interesadas.
- Garantizar la asignación de los recursos humanos, tecnológicos y financieros necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI y del MSPI.
- Integrar los objetivos de seguridad de la información en la planeación estratégica institucional de INVAMA.
- Presidir o delegar la presidencia del Comité Institucional de Gestión y Desempeño, que asume las funciones de gobierno del SGSI en INVAMA.
- Revisar periódicamente los resultados del SGSI y tomar decisiones estratégicas orientadas a su mejora continua.
- Promover una cultura organizacional que valore la seguridad de la información como un habilitador del cumplimiento misional y de la confianza ciudadana.
- Aprobar el mapa de riesgos de seguridad de la información y los niveles de riesgo residual aceptados para la entidad.
- Garantizar el cumplimiento de los reportes de seguridad digital al FURAG en el marco del MIPG.

7- ALCANCE

La implementación del SGSI de INVAMA, conforme a los requisitos de la Resolución MinTIC 02277 de 2025 y la norma ISO/IEC 27001:2022, comprende:

- La totalidad de los procesos misionales y de apoyo del Instituto de Valorización de Manizales — INVAMA.
- Todos los sistemas de información, plataformas tecnológicas, bases de datos, aplicaciones e infraestructura tecnológica de la entidad, independientemente de su ubicación física o modalidad de hospedaje (local, nube o híbrido).

- Los activos de información propios o bajo custodia de INVAMA, en cualquier formato: digital o físico.
- Las instalaciones físicas de INVAMA en Manizales, Caldas, y cualquier ubicación desde la que se realice trabajo remoto autorizado o se presten servicios institucionales.
- Las relaciones con proveedores, contratistas y terceros que accedan, procesen, almacenen o transmitan información institucional de INVAMA.

8- APLICABILIDAD

La presente política, sus objetivos y todos los documentos derivados o complementarios (*manuales, procedimientos, instructivos y formatos del SGSI*) *aplican de forma obligatoria a:*

- Servidores públicos de carrera administrativa y de libre nombramiento y remoción de INVAMA.
- Contratistas de prestación de servicios, consultores e interventores vinculados a INVAMA mediante cualquier modalidad contractual.
- Aprendices, pasantes y estudiantes en práctica que desarrollen actividades en INVAMA.
- Proveedores de servicios tecnológicos, de soporte y de cualquier otra naturaleza que accedan a información, sistemas o instalaciones de INVAMA.
- Personal de entidades externas en comisión o en misión en INVAMA.
- Ciudadanos y terceros en la medida en que interactúen con los sistemas, datos o servicios de INVAMA.

9- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – ROLES Y RESPONSABILIDADES

INVAMA, define los roles y responsabilidades para la implementación del MSPI aprobados por el Comité de Gestión y Desempeño Institucional, mediante acta 01 del 17-04-2023 y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Planes, Procedimientos, Manuales, Formatos, entre otros):

Rol / Instancia / Dependencia	Responsabilidades principales en el SGSI	Funcionario Responsable
Alta Dirección	Aprobar la política de seguridad y sus revisiones. Garantizar los recursos para el SGSI. Presidir el Comité Institucional de Gestión y Desempeño en sus funciones de seguridad. Aprobar el mapa de riesgos y los riesgos residuales aceptados. Declarar la activación del BCP y DRP ante situaciones de desastre.	Gerente General

Rol / Instancia / Dependencia	Responsabilidades principales en el SGSI	Funcionario Responsable
Comité Institucional de Gestión y Desempeño	Asumir las funciones de Comité de Seguridad de la Información en INVAMA. Revisar y aprobar políticas, riesgos y planes del SGSI. Hacer seguimiento a los indicadores de seguridad. Comunicar la importancia de la seguridad de la información a toda la entidad. Revisar los resultados del FURAG en seguridad digital.	Líderes de Unidad
Responsable de Seguridad y Privacidad de la Información y Protección de Datos Personales (RSI)	Diseñar, implementar, operar y mejorar el SGSI de INVAMA. Elaborar y actualizar las políticas, procedimientos y controles de seguridad. Liderar la gestión de riesgos, la gestión de incidentes y las auditorías de seguridad. Actuar como Oficial de Protección de Datos Personales. Coordinar el reporte FURAG y los indicadores del SGSI. Asesorar al Comité Institucional de Gestión y Desempeño en temas de seguridad.	Técnico Administrativo Sistemas
Responsable de Tecnologías de la Información (TI)	Implementar los controles técnicos de seguridad en la infraestructura de INVAMA. Gestionar el control de acceso lógico, las copias de seguridad, el antimalware y el monitoreo de eventos. Ejecutar el hardening, la gestión de vulnerabilidades y parches. Administrar los dispositivos móviles institucionales (MDM). Soportar técnicamente la ejecución del DRP.	Profesional Universitario Sistemas
Gestión del Talento Humano	Incorporar los requisitos de seguridad en los procesos de selección, vinculación y desvinculación. Coordinar la inducción en seguridad de la información para nuevos servidores y contratistas. Notificar oportunamente al RSI y TI sobre cambios de rol y desvinculaciones. Gestionar el proceso disciplinario por incumplimiento de políticas de seguridad.	Profesional Universitario Gestión Humana
Control Interno	Incluir la seguridad de la información en el plan anual de auditorías institucionales. Apoyar al RSI en situaciones de posibles violaciones a las políticas de seguridad. Verificar el cumplimiento de los controles del SGSI en las auditorías. Reportar hallazgos de seguridad al Comité Institucional de Gestión y Desempeño.	Asesor Control Interno
Oficina Jurídica y Contratación	Incorporar cláusulas de seguridad de la información y protección de datos en contratos con proveedores y contratistas. Verificar el cumplimiento de los requisitos	Líder Unidad

Rol / Instancia / Dependencia	Responsabilidades principales en el SGSI	Funcionario Responsable
	legales de seguridad en la gestión contractual. Asesorar al RSI en el reporte de incidentes que involucren datos personales ante la SIC. Apoyar los procesos disciplinarios y penales derivados de violaciones de seguridad.	Jurídica
Líderes de Proceso / Jefes de Dependencia	Implementar las políticas y controles de seguridad en su dependencia. Identificar, declarar y gestionar los activos de información a su cargo. Aprobar las solicitudes de acceso a sistemas e información de su área. Reportar incidentes y eventos de seguridad al RSI oportunamente. Participar en el análisis de riesgos de sus procesos.	Líderes de Unidad
Área de Comunicaciones / Prensa	Apoyar las campañas de sensibilización y cultura en seguridad de la información. Difundir comunicaciones institucionales sobre seguridad en todos los niveles. Gestionar los canales oficiales de INVAMA en redes sociales conforme a las políticas de seguridad.	Profesional Universitario Comunicaciones
Servidores públicos, contratistas y terceros (usuarios)	Conocer, entender y cumplir las políticas de seguridad de la información de INVAMA. Usar los recursos tecnológicos exclusivamente para actividades institucionales autorizadas. Reportar inmediatamente cualquier incidente o evento de seguridad al RSI o TI. Proteger las credenciales de acceso y la información institucional bajo su custodia.	

10- LINEAMIENTOS GENERALES DE CUMPLIMIENTO

Las responsabilidades frente a la seguridad y privacidad de la información son compartidas, definidas, publicadas y de obligatorio cumplimiento para todos los actores del alcance. INVAMA adopta los siguientes lineamientos generales, desarrollados en detalle en el Manual de Políticas Específicas de Seguridad y Privacidad de la Información:

- INVAMA protegerá la información generada, procesada, transmitida o resguardada por sus procesos de negocio, garantizando los principios de confidencialidad, integridad y disponibilidad conforme al nivel de clasificación de cada activo.
- INVAMA implementará controles de acceso lógico y físico a la información, sistemas e infraestructura tecnológica, aplicando el principio de mínimo privilegio y la autenticación multifactor en los sistemas críticos.

- INVAMA protegerá su infraestructura tecnológica crítica mediante controles de seguridad perimetral, gestión de vulnerabilidades, configuración segura y monitoreo continuo de eventos de seguridad.
- INVAMA gestionará los riesgos de seguridad de la información de manera sistemática, conforme a una metodología aprobada, con revisión periódica del mapa de riesgos y planes de tratamiento documentados.
- INVAMA garantizará que la seguridad de la información sea parte integral del ciclo de vida de los sistemas: desde su adquisición o desarrollo hasta su disposición final.
- INVAMA gestionará de forma eficaz los incidentes de seguridad de la información, asegurando la detección oportuna, la respuesta coordinada, la preservación de evidencias y el reporte a las autoridades competentes en los plazos legales establecidos.
- INVAMA garantizará la continuidad de sus procesos misionales ante interrupciones mediante Planes de Continuidad del Negocio (BCP) y de Recuperación ante Desastres (DRP), probados periódicamente. El Comité de Crisis se activa exclusivamente ante la ejecución del DRP.
- INVAMA protegerá los datos personales de ciudadanos, funcionarios y contratistas conforme a los principios de la Ley 1581 de 2012, garantizando el ejercicio de los derechos de los titulares y el cumplimiento de las obligaciones del Responsable del Tratamiento ante la SIC.
- INVAMA gestionará de manera segura las relaciones con proveedores y contratistas, incorporando requisitos de seguridad de la información en los procesos de contratación y supervisando su cumplimiento durante la ejecución.
- INVAMA garantizará el cumplimiento de sus obligaciones de reporte al FURAG en el componente de seguridad digital del MIPG, manteniendo evidencias documentadas y verificables de la implementación del SGSI.
- El incumplimiento de la presente política o de sus documentos derivados genera las consecuencias disciplinarias, civiles y penales establecidas en el marco normativo colombiano vigente.

11- ACCIONES ESTRATEGICAS PARA LA IMPLEMENTACIÓN

Componente	Acción Estratégica
Proteger los activos de información	Elaborar y mantener actualizado el inventario de activos de información institucionales, asignando propietario y nivel de clasificación a cada activo, conforme al Manual de Políticas Específicas.
Gestionar los riesgos de seguridad	Realizar anualmente el análisis y evaluación de riesgos de seguridad de la información de todos los procesos de INVAMA, actualizando el mapa de riesgos y el Plan de Tratamiento de Riesgos con base en los resultados obtenidos.
Garantizar la protección de	Mantener actualizado el Registro Nacional de Bases de Datos (RNBD) ante la SIC, elaborar y publicar el Aviso de Privacidad institucional y establecer el

Componente	Acción Estratégica
datos personales	canal de atención de solicitudes de titulares.
Fortalecer la cultura de seguridad	Diseñar y ejecutar anualmente el Plan de Capacitación y Sensibilización en Seguridad de la Información, diferenciado por rol, con evaluación de efectividad y registro de evidencias.
Cumplir el marco normativo	Mantener una matriz de requisitos legales y normativos actualizada, realizar revisiones semestrales de cumplimiento y reportar oportunamente los indicadores del SGSI en el FURAG dentro de los plazos del ciclo MIPG.
Gestionar eficazmente los incidentes	Implementar y mantener operativo el proceso de gestión de incidentes de seguridad, incluyendo el canal oficial de reporte, el registro centralizado de incidentes y los protocolos de notificación a la SIC y demás autoridades competentes.
Garantizar la continuidad operacional	Elaborar, probar y actualizar anualmente el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP), asegurando que los procesos críticos de INVAMA puedan recuperarse dentro de los tiempos definidos.
Controlar el acceso a información y sistemas	Implementar el proceso formal de gestión del ciclo de vida de accesos (solicitud, aprobación, creación, revisión y revocación), aplicando autenticación multifactor en los sistemas críticos y revisando los perfiles de acceso de forma semestral.
Asegurar las relaciones con proveedores	Incorporar cláusulas de seguridad de la información en el 100% de los contratos con proveedores que accedan a información o sistemas de INVAMA, y realizar seguimiento semestral al cumplimiento de dichos requisitos durante la ejecución contractual.
Mejorar continuamente el SGSI	Ejecutar el programa anual de auditorías internas de seguridad, presentar los resultados al Comité de Gestión y Desempeño Institucional, y gestionar los planes de mejoramiento derivados con seguimiento trimestral.

12. PLAN DE ACCION, SEGUIMIENTO Y EVALUACIÓN

Acción Estratégica	Responsable	Periodicidad	Indicador de Seguimiento	Meta

Acción Estratégica	Responsable	Periodicidad	Indicador de Seguimiento	Meta
Inventario de activos actualizado	RSI + Propietarios de activos	Anual / Ante cambios	% activos con propietario y clasificación asignada	100%
Análisis y mapa de riesgos actualizado	RSI	Anual	Mapa de riesgos aprobado por el Comité de Gestión	1 vez/año
RNBD, Aviso de Privacidad y canal de titulares operativo	RSI	Permanente / Actualización ante cambios	RNBD actualizado + canal publicado	100%
Plan de Capacitación ejecutado	RSI + Gestión Humana	Anual	% personal capacitado en seguridad	≥ 85%
Reporte FURAG diligenciado en plazo	RSI	Anual (según calendario DNP/MinTIC)	Reporte enviado dentro del plazo oficial	100%
Canal de reporte de incidentes operativo y registro actualizado	RSI	Permanente	% incidentes registrados y cerrados con informe	100%
BCP y DRP probados	RSI + Área de TI	Anual	Prueba realizada con informe documentado	1 prueba/año
Revisión semestral de perfiles de acceso	RSI + Área de TI	Semestral	Informe de revisión de privilegios	2 veces/año
Contratos con	Oficina Jurídica	Por cada contrato	% contratos con	100%

Acción Estratégica	Responsable	Periodicidad	Indicador de Seguimiento	Meta
cláusulas de seguridad	+ RSI		cláusulas de seguridad incorporadas	
Auditoría interna del SGSI ejecutada	RSI + Control Interno	Anual	Informe de auditoría con plan de mejoramiento	1 auditoría/año

13. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

INVAMA realiza el seguimiento y evaluación del SGSI mediante los siguientes mecanismos:

- Revisión periódica de los indicadores de gestión del SGSI con frecuencia mínima *trimestral*.
- Auditorías internas de seguridad de la información al menos una (1) vez al año, coordinadas por el RSI y apoyadas por la Oficina de Control Interno.
- Revisión por la Alta Dirección del estado del SGSI al menos una (1) vez al año, en el marco del Comité Institucional de Gestión y Desempeño.
- Reporte anual de avances del SGSI en el Formulario Único de Reporte de Avances de la Gestión (FURAG), en el componente de seguridad digital de la dimensión de Gestión de Tecnologías de la Información del MIPG.
- Evaluación de la efectividad de los controles implementados mediante ejercicios de prueba de penetración, simulacros de phishing y pruebas del DRP, con frecuencia al menos anual.
- Seguimiento trimestral al Plan de Tratamiento de Riesgos de Seguridad de la Información, con reporte al Comité Institucional de Gestión y Desempeño.

14. COMUNICACIÓN

La Política General de Seguridad y Privacidad de la Información del Instituto de Valorización de Manizales — INVAMA será publicada, difundida y socializada a todos los servidores públicos, contratistas y demás colaboradores de la entidad, garantizando su conocimiento, apropiación y aplicación en el desarrollo de las funciones institucionales, así como en el tratamiento adecuado de los activos de información institucionales y los datos personales de los ciudadanos.

Para ello, INVAMA implementará diferentes mecanismos de comunicación que permitan asegurar la comprensión y cumplimiento de los lineamientos establecidos, entre los cuales se destacan:

- Publicación oficial en los medios institucionales de INVAMA, incluyendo la página web oficial y el repositorio documental del Sistema de Gestión de Calidad.
- Difusión por correo electrónico corporativo, dirigida a todos los servidores públicos, contratistas, pasantes y demás colaboradores de la entidad, al momento de la aprobación de la política y ante cada actualización de la misma.
- Socialización a cargo del Responsable de Seguridad de la Información (RSI), en coordinación con la Oficina Asesora de Planeación y Calidad y el área de Gestión Humana, dirigida a todos los niveles de la organización.
- Inclusión de los lineamientos de la política en el proceso de inducción y reinducción institucional, garantizando que todo servidor público o contratista conozca sus obligaciones en materia de seguridad de la información antes de acceder a los sistemas y activos institucionales.
- Actividades de sensibilización y capacitación periódicas que permitan fortalecer las competencias del personal en materia de seguridad de la información, privacidad de datos personales, gestión de incidentes y uso seguro de los recursos tecnológicos institucionales.
- Comunicaciones internas dirigidas a grupos específicos según su rol y nivel de acceso a la información, diferenciando los mensajes para usuarios finales, líderes de proceso, personal de TI y Alta Dirección.

La Oficina Asesora de Planeación y Calidad, en articulación con el Responsable de Seguridad de la Información y el área de Gestión Humana, será responsable de coordinar las actividades de comunicación y difusión de la presente política, así como de verificar que la información divulgada sea clara, accesible, esté permanentemente actualizada y llegue a la totalidad de las partes interesadas definidas en el alcance de la política.

15. POLITICAS CON LAS QUE INTERACTUA

La presente Política Institucional de Gestión Documental se articula e interactúa con las demás políticas institucionales que conforman el Modelo Integrado de Planeación y Gestión – MIPG, en cumplimiento del Decreto 1499 de 2017 y de los lineamientos expedidos por el Departamento Administrativo de la Función Pública (DAFP). Estas políticas, de carácter transversal, buscan fortalecer la eficiencia administrativa, la transparencia, la sostenibilidad y la mejora continua de la gestión pública en el Instituto de Valorización de Manizales – INVAMA. Entre las principales políticas con las que interactúa se encuentran:

Dimensión 1 — Talento Humano

Política de Gestión Estratégica del Talento Humano La seguridad de la información interactúa en los procesos de selección (verificación de antecedentes), inducción (formación en seguridad antes del primer acceso a sistemas), capacitación (plan anual de sensibilización en seguridad) y desvinculación (revocación de accesos y paz y salvo de seguridad). Los perfiles de cargo deben incluir las competencias y responsabilidades de seguridad asociadas al rol.

Dimensión 2 — Direccionamiento Estratégico y Planeación

Política de Planeación Institucional Los objetivos del SGSI de INVAMA deben estar articulados con el Plan de Acción institucional y el Plan Estratégico. Los recursos para la implementación del SGSI se planean dentro del proceso de planeación anual. Los indicadores del SGSI se integran al tablero de control institucional.

Política de Gestión del Riesgo Esta es la interacción más directa. La gestión de riesgos de seguridad de la información se articula con la metodología institucional de gestión del riesgo del DAFP y se refleja en el mapa de riesgos institucional de INVAMA. Los riesgos de seguridad digital hacen parte del mapa de riesgos de corrupción y de gestión.

Dimensión 3 — Gestión con Valores para Resultados

Política de Fortalecimiento Organizacional y Simplificación de Procesos La seguridad de la información debe considerarse en el diseño y rediseño de procesos institucionales, garantizando que los controles de seguridad no generen cargas innecesarias pero sí protejan la información que fluye por cada proceso.

Política de Gobierno Digital Es la interacción más estrecha dentro de esta dimensión. La seguridad y privacidad de la información es uno de los habilitadores transversales del Marco de Referencia de Arquitectura Empresarial y del componente de Gobierno Digital del MIPG. El MSPI (Resolución MinTIC 02277 de 2025) es parte integral de la Política de Gobierno Digital. El reporte FURAG de seguridad digital se hace dentro de esta política.

Política de Seguridad Digital En el MIPG, la Seguridad Digital es una política específica que se nutre directamente de la Política General de Seguridad y Privacidad de la Información de INVAMA. Ambas son la misma materia vista desde el marco institucional (MIPG) y el marco técnico (SGSI/MSPI). El reporte FURAG del componente de seguridad digital corresponde a esta política.

Política de Defensa Jurídica Interactúa en los incidentes de seguridad que deriven en procesos judiciales o administrativos, en la gestión de violaciones de datos personales ante la SIC, y en la incorporación de cláusulas de seguridad en contratos y convenios.

Dimensión 4 — Evaluación de Resultados

Política de Seguimiento y Evaluación del Desempeño Institucional Los indicadores del SGSI forman parte del sistema de seguimiento y evaluación de INVAMA. Los resultados del SGSI se reportan al FURAG y alimentan el proceso de evaluación del desempeño institucional en el componente de Gobierno Digital.

Dimensión 5 — Información y Comunicación

Política de Transparencia, Acceso a la Información y Lucha contra la Corrupción La seguridad de la información interactúa directamente con esta política en dos sentidos: (1) la clasificación de la información (pública, interna, confidencial, reservada) conforme a la Ley 1712 de 2014 determina qué información debe publicarse y cuál debe protegerse; (2) los controles de trazabilidad, logs de auditoría y gestión de accesos son mecanismos que apoyan la transparencia y la lucha contra la corrupción.

Política de Comunicaciones La seguridad en las comunicaciones institucionales (correo electrónico, internet, redes sociales, videoconferencias) impacta directamente la gestión de las comunicaciones de INVAMA. Los canales de comunicación deben cumplir los controles de seguridad definidos en el SGSI.

Política de Gestión Documental Interactúa en los plazos de retención de información, la disposición final segura de documentos (borrado seguro, destrucción física), la protección de

archivos físicos con información confidencial y el manejo de documentos electrónicos con firma digital.

Dimensión 6 — Gestión del Conocimiento y la Innovación

Política de Gestión del Conocimiento y la Innovación El conocimiento sobre el SGSI, las *lecciones aprendidas de incidentes de seguridad y las buenas prácticas identificadas deben* gestionarse y transferirse dentro de INVAMA como parte del conocimiento institucional. La innovación tecnológica y la transformación digital deben incorporar los principios de seguridad por diseño desde su concepción.

Dimensión 7 — Control Interno

Política de Control Interno El Sistema de Control Interno de INVAMA incluye las auditorías al SGSI dentro de su programa anual. La Oficina de Control Interno evalúa el cumplimiento de las políticas de seguridad y reporta sus hallazgos al Comité de Gestión y Desempeño. Los controles del SGSI son complementarios a los controles del Sistema de Control Interno Contable (SCIC).

16. RESPONSABLES DE SU IMPLEMENTACIÓN

Por la naturaleza, misionalidad y objetivo de la Política General de Seguridad y Privacidad de la Información, el Responsable de Seguridad y Privacidad de la Información y Protección de Datos Personales (RSI) del Instituto de Valorización de Manizales — INVAMA será el responsable de su divulgación, sensibilización para su implementación y cumplimiento de su plan de acción.

Sin perjuicio de lo anterior, y dado el carácter transversal de la seguridad de la información en todos los procesos institucionales, la implementación efectiva de esta política requiere la participación activa y coordinada de las siguientes dependencias y roles:

El **área de Gestión Humana** es responsable de garantizar que los lineamientos de seguridad de la información se incorporen en los procesos de selección, inducción, capacitación y desvinculación del personal, asegurando que todo servidor público y contratista conozca sus obligaciones antes de acceder a los sistemas y activos institucionales de INVAMA.

El **área de Tecnologías de la Información** es responsable de implementar los controles técnicos de seguridad en la infraestructura tecnológica de INVAMA, gestionar el acceso lógico a los sistemas de información y ejecutar las acciones operativas del plan de acción del SGSI bajo la supervisión del RSI.

La **Oficina de Planeación y Calidad** es responsable de articular los objetivos e indicadores del SGSI con el Plan de Acción institucional, coordinar las actividades de comunicación y difusión de la política y apoyar el proceso de reporte al FURAG en el componente de seguridad digital del MIPG.

La **Oficina Jurídica** es responsable de incorporar las cláusulas de seguridad de la información y confidencialidad en los contratos y órdenes de servicio con proveedores y contratistas, y de asesorar en el cumplimiento del marco legal aplicable al SGSI de INVAMA.

La **Oficina de Control Interno** es responsable de incluir la seguridad de la información en su programa anual de auditorías, verificar el cumplimiento de los lineamientos de esta política y reportar los hallazgos al Comité de Gestión y Desempeño Institucional para la adopción de planes de mejoramiento.

Los **líderes de proceso** son responsables de garantizar el cumplimiento de los lineamientos de seguridad de la información en sus respectivas dependencias, declarar los activos de información a su cargo y reportar oportunamente al RSI cualquier incidente o evento de seguridad detectado.

Todos los **servidores públicos, contratistas y demás colaboradores** de INVAMA son responsables de conocer, apropiar y cumplir los lineamientos de la presente política y los documentos derivados del SGSI en el desarrollo de sus funciones institucionales, independientemente de su cargo, nivel jerárquico o modalidad de vinculación. El uso indebido de ésta política puede ocasionar consecuencias de tipo legal.

17. REVISIÓN Y APROBACIÓN

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 (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.

Esta política fue aprobada mediante Acta No. 005 del 10-01-2026 Comité Institucional de Gestión y Desempeño.

Firma

JORGE MANUEL GARCIA MONTES
Gerente