Plan de Seguridad y Privacidad de la Información

2026

Instituto de Valorización de Manizales

INVAMA

Manizales, enero de 2026

Versión 6.0

CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

1. INTRODUCCIÓN

El presente Plan de Seguridad y Privacidad de la Información (PSPI) establece las directrices, lineamientos y acciones que la Entidad adoptará para proteger la información y los datos personales bajo su custodia, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información, en cumplimiento del Decreto 612 de 2018 y la Política de Gobierno Digital.

Este plan se formula como instrumento de planeación institucional y se integra al Modelo Integrado de Planeación y Gestión – MIPG, articulándose con el Modelo de Seguridad y Privacidad de la Información – MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, así mismo, define las acciones prioritarias para consolidar el MSPI, cerrar brechas identificadas y fortalecer la cultura de seguridad y privacidad en la entidad.

El Plan de Seguridad y Privacidad de la Información se articula con el Modelo Integrado de Planeación y Gestión (MIPG), específicamente con la Dimensión de Gobierno Digital y el componente de Seguridad Digital, evaluado a través del Formulario Único de Reporte de Avances de la Gestión (FURAG).

Las actividades definidas en el PSPI permiten evidenciar el cumplimiento de los criterios evaluados en FURAG, tales como:

- Existencia y actualización del PSPI.
- Implementación del MSPI.
- Gestión de riesgos de seguridad digital.
- Protección de datos personales.
- Gestión de incidentes de seguridad.
- Continuidad del negocio.

2. OBJETIVOS

2.1 Objetivo General

Establecer las acciones estratégicas, técnicas y administrativas necesarias para gestionar adecuadamente la seguridad y privacidad de la información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital.

2.2 Objetivos Específicos

- Proteger los activos de información críticos de la Entidad.
- Garantizar el cumplimiento de la normatividad vigente en seguridad de la información y protección de datos personales.
- Implementar controles de seguridad acordes con los riesgos identificados.
- Fortalecer la cultura organizacional en seguridad y privacidad de la información.
- Establecer mecanismos de seguimiento y mejora continua del MSPI.

3. ALCANCE

El Plan Estratégico de Seguridad de la Información – PSPI aplica a todos los procesos, funcionarios, contratistas, terceros, sistemas de información, bases de datos, infraestructura tecnológica y activos de información de la Entidad, independientemente de su formato o medio de almacenamiento, con énfasis en información clasificada, reservada y datos personales.

4. MARCO NORMATIVO

- **Constitución Política de Colombia. Art. 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. **Art 20.** Tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. **Art. 209.** La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones. Las autoridades administrativas deben coordinar sus actuaciones para el adecuado cumplimiento de los fines del Estado. La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley. **Art. 269.** En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas.
- **Ley 527 de 1999.** Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información.
- **Ley 599 de 2000**: Código Penal**.** Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
- **Ley 1266 de 2008**. Disposiciones generales del Hábeas Data y se regula el manejo de la información. Por la cual se dictan 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 1221 de 2008**. Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Código Penal. 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 se preservan integralmente los sistemas que utilicen las tecnologías de la información

y las comunicaciones, entre otras disposiciones. Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.

- **Ley 1341 de 2009.** Sociedad de la Información y las Tecnologías de la Información y Comunicaciones (TIC).
- **CONPES 3701 de 2011.** Lineamientos de Política para la Ciberseguridad y Ciberdefensa. Busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
- **Ley 1581 de 2012. Protección de Datos Personales.** Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
- **Decreto 2609 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Resolución 3933 de 2013 del Ministerio de Defensa Nacional.** Crea y organiza grupos internos de trabajo. Creó el Grupo ColCERT y asignó funciones a la dependencia de La Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
- **Ley 1712 de 2014**. Ley de transparencia y del derecho de acceso a la información pública Nacional y se dictan otras disposiciones.
- **Decreto 886 de 2014**. Por el cual se reglamenta el Registro Nacional de Bases de Datos
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- **Decreto 1078 de 2015**. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1080 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 1083 de 2015.** establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital. Fortalece las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
- **Decreto 1499 de 2017**. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 090 de 2018.** Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
- **Decreto 1008 de 2018**. Establecen los lineamientos generales de la política de Gobierno Digital bajo los principios de innovación, competitividad, proactividad y seguridad de la información.
- **Ley 1928 de 2018.** Convenio sobre la ciberdelincuencia. Se aprueba el convenio sobre la ciberdelincuencia adoptado el 23 de noviembre de 2001, en Budapest. Tiene por objeto la materialización de una política criminal común en materia de ciberdelincuencia mediante la adopción de lineamientos.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **CONPES 3920 de 2018.** Política Nacional de Explotación de Datos (Big Data). El propósito central de esta política es aumentar el aprovechamiento de datos en Colombia, mediante el desarrollo de condiciones para que estos sean gestionados como activos generadores de valor social y económico en el país. Esta política ha habilitado el uso intensivo de datos y su aprovechamiento en Colombia.
- **Decreto 2106 de 2019**. Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos

que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario.
- **Decreto 2106 de 2019.** Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- **CONPES 3975 de 2019**. Política Nacional para la Transformación Digital e Inteligencia Artificial. Plantea las condiciones para potenciar la generación de valor social y económico en Colombia a través del uso estratégico de tecnologías digitales de manera amplia, involucrando al sector público y el sector privado con énfasis en el uso de las TIC como herramientas para impulsar la productividad y favorecer el bienestar de los ciudadanos, quienes son los beneficiarios y consumidores de los bienes y servicios que se producen. Así mismo, busca que se den las condiciones necesarias para el impulso de la IA como uno de los aceleradores más importantes de este proceso en la actualidad, sin desconocer el potencial de otras tecnologías digitales. Todo lo anterior con el objetivo de aprovechar las oportunidades y enfrentar los retos relacionados con la 4RI.
- **Decreto 620 de 2020**. Por el cual se subroga el Título 17 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **Decreto 1287 de 2020**. Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.** Formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.
- **Ley 2088 de 2021.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- **Ley 2166 de 2021.** Por medio de la cual se fortalecen las medidas de protección a la infraestructura crítica cibernética.
- **Directiva Presidencial 03 de 2021**. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- **Resolución 500 de 2021.** Lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Directiva Presidencial 02 de 2022.** Reiteración de la política pública en materia de seguridad digital.
- **Decreto 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- **Decreto 338 de 2022.** Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
- **Resolución 746 de 2022**. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen los lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
- **Resolución 460 de 2022.** Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales de su implementación.
- **Decreto 767 de 2022**. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1263 de 2022.** Adiciona un Título al Decreto 1078 de 2015, sobre los lineamientos y estándares de transformación digital, de la Administración Pública en el marco de la Política de Gobierno Digital, así mismo, define las expresiones para la interpretación del presente título, las expresiones aquí utilizadas deben ser entendidas con el significado que se establece en la misma norma, tales como, Transformación Digital, Inteligencia artificial, Lineamientos y Estándares para la Transformación Digital de la Administración Pública, Uso de la infraestructura de datos, etc.
- **CONPES 4144 de 2025**. Política Nacional de Inteligencia Artificial.
- **Resolución 0227 de 2025.** Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- **Norma Internacional NTC ISO 27001.** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

- **Norma Internacional NTC ISO 27002.** Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
- **Norma Internacional NTC ISO 27005.** Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de los riesgos de seguridad de la información
- **Norma Internacional NTC ISO 31000.** Administración / Gestión de riesgos – Lineamientos guía.
- **Norma Internacional GDPR (Reglamento General de Protección de Datos):** prácticas con derechos del titular, principios de minimización, portabilidad, notificación de brechas de seguridad y consentimiento explícito, como complemento a la Ley 1581 de 2012.
- **Norma Internacional NIST SP 800-53:** Guía técnica para complementar los controles de seguridad del MSPI, especialmente en sistemas críticos o servicios de procesamiento masivo de datos.

5. GLOSARIO

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **ARCO:** Derechos de Acceso, Rectificación, Cancelación y Oposición en tratamiento de datos personales.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior. (ArCert)

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- **BIA:** Business Impact Analysis - Análisis de Impacto al Negocio.

- **Cifrado:** Proceso de transformar información usando un algoritmo para hacerla ilegible sin conocimiento de la clave.

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000)

- **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. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente

ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000).

- **DRP:** Disaster Recovery Plan - Plan de Recuperación ante Desastres.

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Incidente de seguridad:** Evento adverso confirmado o serie de eventos relacionados, que tienen una probabilidad alta de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000).

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

- **KPI:** Key Performance Indicator - Indicador Clave de Desempeño.

- **Logs:** Registros de eventos de un sistema de información.

- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **No repudio:** El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. También se puede definir como el servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO/IEC 27000).

- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **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.

- **Registro Nacional de Bases de Datos - RNBD:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI:** 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. (ISO/IEC 27000).

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

6. DIAGNÓSTICO DE LA ENTIDAD

Esta etapa de DIAGNÓSTICO según ISO 27001 en el Capítulo 4 - Contexto Organizacional determina la necesidad de analizar los problemas externos e internos del Instituto de Valorización de Manizales – INVAMA - y su contexto, incluye los requisitos y expectativas de las partes interesadas de la organización para lograr el alcance del SGSI.

Figura 1. Etapas previas a la implementación

Fuente: MinTIC, "Modelo de Seguridad y Privacidad de la Información," 2016.

6.1 Metodología del diagnóstico

Esta fase de diagnóstico permite establecer el estado actual de la implementación de la seguridad y privacidad de la información del INVAMA, para tal fin se realiza un diagnóstico utilizando el "Instrumento de Evaluación del MSPI", con el que se identifica los controles implementados y faltantes y así tener insumos fundamentales para las fases de planificación.

La madurez de la seguridad y privacidad de la información del INVAMA incluye los controles tanto administrativos como técnicos, la competencia técnica de los recursos informáticos, los procesos y las prácticas sostenibles, así como la eficiencia de los controles establecidos al interior de la entidad. Para ello se estableció una línea de partida de la madurez de la seguridad con el fin de ser usada para definir los procesos en las que centra las actividades de seguridad de la información de la entidad, el nivel de madurez se identificó mediante el diligenciamiento del Instrumento de Evaluación MSPI, que permitió identificar el estado actual que cuenta la Entidad con respecto al Modelo de Seguridad y Privacidad de la Información y se identificaron requisitos que en su mayoría han sido previamente evaluados.

La Entidad realizó el diagnóstico del estado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) utilizando la herramienta oficial de autodiagnóstico del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, alineada con la Norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información y las mejores prácticas internacionales en gestión de la seguridad de la información **GT-SP-FO-01 Autodiagnóstico MSPI 27001_2022.**

El diagnóstico se desarrolló bajo un enfoque integral, evaluando:

- El grado de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) bajo el ciclo **PHVA (Planear – Hacer – Verificar – Actuar)**.
- La efectividad de los controles definidos en el **Anexo A de la ISO/IEC 27001:2022**.
- La capacidad institucional frente a buenas prácticas de **ciberseguridad**, tomando como referencia el **Marco de Ciberseguridad del NIST (CSF)**.

6.2 Resultados del diagnóstico por componentes del SGSI (Ciclo PHVA)

Como resultado de la evaluación del SGSI bajo el enfoque PHVA, la Entidad alcanzó un nivel de avance general del **65%** frente al 100% esperado, evidenciando avances diferenciados entre los distintos componentes del sistema.

- **Planificación (Contexto de la organización, Liderazgo, Planificación y Soporte):** se evidencian avances cercanos a los niveles esperados, con estructuras básicas de gobernanza, definición de roles y lineamientos generales documentados. No obstante, se identifican oportunidades de mejora en la formalización y actualización de políticas, procedimientos y planes.
- **Implementación (Operación):** presenta un avance intermedio, con controles operativos implementados, aunque con necesidad de fortalecer su estandarización y trazabilidad.
- **Evaluación del desempeño:** se identifican brechas relevantes relacionadas con la definición de indicadores, auditorías internas y seguimiento sistemático al desempeño del SGSI.
- **Mejora continua:** se evidencia un nivel de avance bajo, asociado principalmente a la falta de mecanismos formales y periódicos de revisión por la dirección y acciones de mejora estructuradas.

Estos resultados reflejan un SGSI en fase de consolidación, con bases establecidas, pero con necesidad de fortalecimiento en los procesos de evaluación y mejora.

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado	% de Avance Actual
2025	PLANIFICACIÓN	4. CONTEXTO DE LA ORGANIZACIÓN	12%	14%	85%
		5. LIDERAZGO	12%	14%	87%
		6. PLANIFICACIÓN	10%	14%	73%
		7. SOPORTE	10%	14%	72%
	IMPLEMENTACIÓN	8. OPERACIÓN	10%	16%	60%
	EVALUACIÓN DE DESEMPEÑO	9. EVALUACIÓN DE DESEMPEÑO	7%	14%	47%
	MEJORA CONTINUA	10. MEJORA	4%	14%	30%
TOTAL			65%	100%	65%

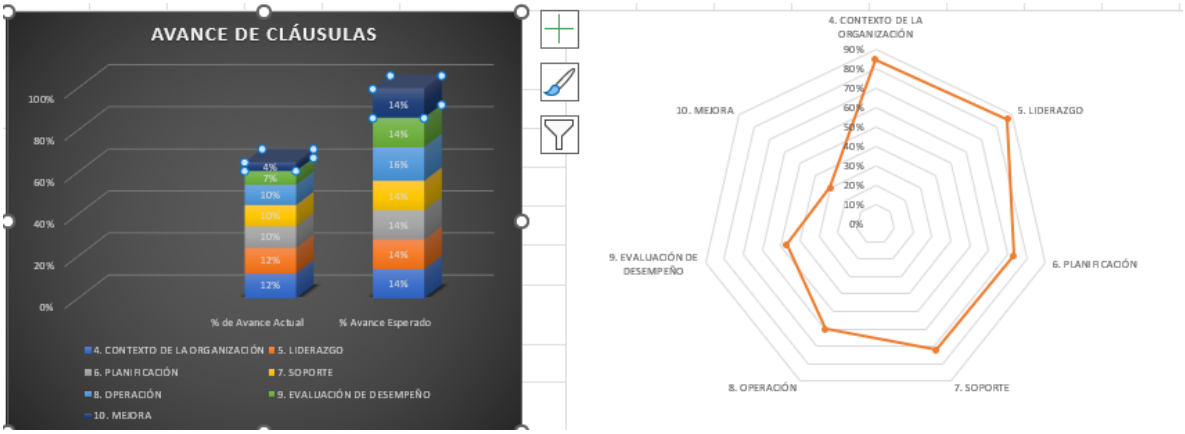

Figura 2. Avance Cláusulas del Modelo de Operación (PHVA)

Fuente: Instrumento de Evaluación MSPI – Dashboard

6.3 Evaluación de efectividad de los controles del Anexo A de la ISO/IEC 27001:2022

La evaluación de la efectividad de los controles definidos en el Anexo A de la ISO/IEC 27001:2022 arrojó un **promedio general de efectividad del 42%**, clasificado en un nivel **efectivo**, con diferencias relevantes entre dominios:

- **A.5 Controles organizacionales:** nivel de madurez **repetible**, con brechas asociadas a la formalización de políticas, procedimientos y estructuras de gobernanza.

- **A.6 Controles de personas:** nivel de madurez **repetible**, evidenciando oportunidades de mejora en capacitación, concienciación y responsabilidades frente a la seguridad y privacidad de la información.
- **A.7 Controles físicos:** nivel de madurez **efectivo**, con controles implementados de forma consistente en las instalaciones y activos físicos.
- **A.8 Controles tecnológicos:** nivel de madurez **efectivo**, con medidas técnicas operativas, aunque con oportunidades de fortalecimiento en monitoreo y gestión preventiva.

Estos resultados permiten priorizar acciones de fortalecimiento en los controles organizacionales y de personas, sin desconocer la necesidad de mejora continua en los controles físicos y tecnológicos.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	38	100	REPETIBLE
A.6	CONTROLES DE PERSONAS	38	100	REPETIBLE
A.7	CONTROLES FÍSICOS	47	100	EFECTIVO
A.8	CONTROLES TECNOLÓGICOS	45	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		42	100	EFECTIVO

Figura 3. Evaluación de efectividad de controles – ISO 27001:2002 Anexo A

Fuente: Instrumento de Evaluación MSPI – Dashboard

6.4 Evaluación frente a mejores prácticas de ciberseguridad (NIST CSF)

De manera complementaria, la Entidad evaluó su nivel de capacidad frente al **Marco de Ciberseguridad del NIST (CSF)**, identificando mayores avances en las funciones de **Gobernar, Identificar y Proteger**, y brechas significativas en las funciones de **Detectar, Responder y Recuperar**.

Lo anterior evidencia la necesidad de fortalecer los procesos relacionados con la detección temprana de incidentes de seguridad, la gestión de incidentes, la continuidad del negocio y los planes de recuperación ante desastres.

MODELO FRAMEWORK CIBERSEGURIDAD		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
GOBERNAR	53	100
IDENTIFICAR	48	100
PROTEGER	58	100
DETECTAR	40	100
RESPONDER	20	100
RECUPERAR	28	100

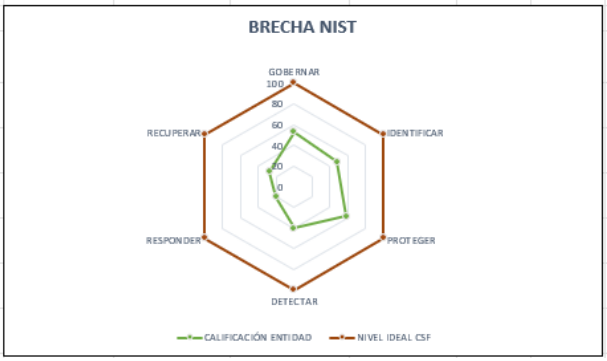

Figura 4. Evaluación frente a mejores prácticas de ciberseguridad (NIST CSF)

Fuente: Instrumento de Evaluación MSPI – Dashboard

6.5 Análisis consolidado de brechas del MSPI

A partir del diagnóstico integral realizado, se identificaron brechas prioritarias asociadas a:

A continuación, se resumen los principales hallazgos por componente:

- **Gobernanza y Organización:** Existen estructuras y comités definidos; sin embargo, se requiere fortalecer su formalización y documentación mediante actos administrativos específicos y socialización institucional, así como la formalización y actualización de políticas, procedimientos y lineamientos de seguridad y privacidad de la información.
- **Identificación y Clasificación de Activos:** La Entidad cuenta con inventarios de activos y esquemas de clasificación definidos, los cuales

deben ser actualizados y complementados con la identificación formal de propietarios y custodios.

- **Gestión de Riesgos:** Se dispone de una metodología adoptada; no obstante, el análisis, valoración y tratamiento de riesgos debe ser actualizado y aprobado formalmente.
- **Controles de Seguridad:** Se han implementado controles básicos administrativos, técnicos y físicos; se identifican oportunidades de mejora en controles avanzados como autenticación multifactor, cifrado y gestión de parches.
- **Privacidad y Protección de Datos Personales:** Se cuenta con políticas y mecanismos de atención a titulares, requiriéndose fortalecer la seguridad técnica de las bases de datos y la actualización del RNBD.
- **Gestión de Incidentes:** El proceso se encuentra definido e implementado, con oportunidades de mejora en capacidades de detección y respuesta, así como la implementación del plan de continuidad del negocio y recuperación ante desastres.
- **Capacitación y Concientización:** Se realizan acciones de capacitación; se requiere estructurar y ejecutar un plan anual integral.
- **Seguimiento y Mejora Continua:** Se identifican debilidades en la definición y seguimiento de indicadores y en la revisión sistemática por la dirección.

Las brechas identificadas constituyen el insumo principal para la formulación y ejecución del Plan de Seguridad y Privacidad de la Información, en concordancia con el Decreto 612 de 2018 y los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

7. PLANIFICACIÓN

7.1 Comprensión de la Organización y de su Contexto

A partir del Acuerdo 013 de 1987 se crea el Instituto de Valorización de Manizales - INVAMA- como un establecimiento público de carácter municipal, con autonomía administrativa, personería jurídica y patrimonio propio e independiente; sujeto a los derechos inherentes de las personas jurídicas de derecho público de acuerdo a las normas generales y le corresponde como organismo descentralizado del Municipio de Manizales, los derechos de éste para atender a la función pública comprendida dentro de su objeto:

- La ejecución de obras de interés público por el sistema de la contribución de valorización.
- La prestación del servicio de alumbrado público a través de la administración, mantenimiento, expansión y cualquier tipo de operación inmerso en el servicio.
- El diseño, comercialización, mantenimiento y ejecución del alumbrado navideño de Manizales.
- La prestación de asesorías relacionadas con el objeto misional (valorización y alumbrado público) a otros municipios o entidades públicas.

A. **Misión de la Entidad. En INVAMA,** nos dedicamos a generar progreso y bienestar a las comunidades a través de la implementación, desarrollo y ejecución de obras de infraestructura por el sistema de contribución por valorización y los servicios de alumbrado público, impulsando la innovación y el uso eficiente de la energía. Estamos enfocados en fomentar el desarrollo sostenible, a través de prácticas que respeten el medio ambiente y promuevan la inclusión social. Nuestras acciones se fundamentan en los principios de excelencia, transparencia y colaboración.

B. **Visión de la Entidad.** Para el 2034, INVAMA continuará como líder y referente regional en el desarrollo de proyectos de infraestructura por el sistema de contribución de valorización y la prestación de servicios de alumbrado público, generando progreso y calidad de vida para nuestras comunidades, implementando la innovación y sostenibilidad en todas nuestras prácticas. A nivel nacional será referente en la prestación de servicios de asesoría para la implementación de proyectos por contribución de valorización y alumbrados públicos.

C. **Estructura Organizacional.** Tal como se puede apreciar en la *Figura 4* se presenta la estructura organizacional del INVAMA de acuerdo al acuerdo número 004 del 28 de octubre de 2018.

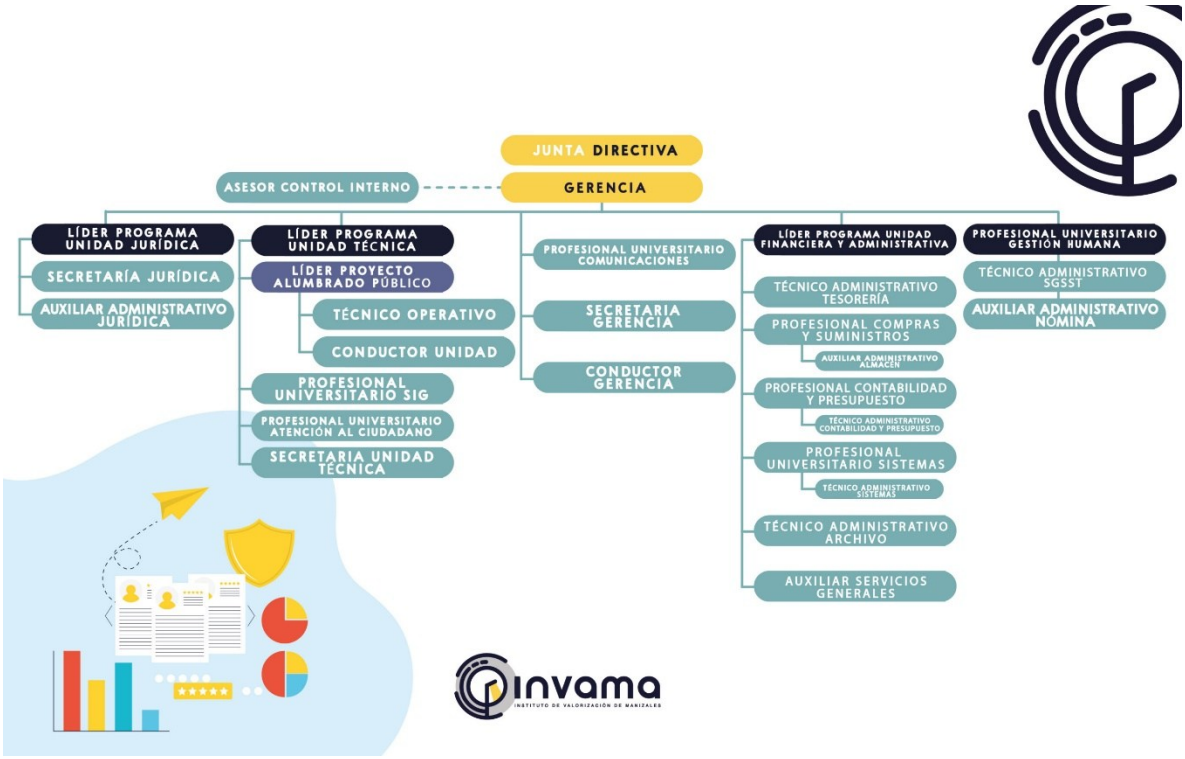

Figura 5. Estructura Organizacional de INVAMA

Fuente: INVAMA

D. **Mapa de Procesos.** INVAMA se encuentra estructurada por procesos, tal como se puede apreciar en la *figura 5* se definen en procesos estratégicos, misionales, apoyo y evaluación y control, en la *tabla* 1 podemos apreciar la descripción de cada proceso.

Figura 6. Mapa de Procesos de INVAMA

Fuente: INVAMA

Tabla 1. Descripción de Procesos INVAMA

Tipo	Proceso	Objetivo
Estratégico	Direccionamiento estratégico y planeación	Definir las estrategias, objetivos, metas, planes de acción, procesos y procedimientos adecuados, políticas operacionales y niveles de responsabilidad,

		mecanismos de mitigación de riesgos e implementar la mejora continua.
Misionales	Alumbrado Público	Prestar de manera óptima el servicio de alumbrado público y velar por el uso eficiente de los recursos y el mantenimiento de la infraestructura que lo compone, además de prestar servicios de asesoría en condiciones de calidad y oportunidad para los municipios que lo requieran.
Misionales	Proyectos de Valorización	Determinar la viabilidad de construir obras públicas mediante el Sistema de Contribución de Valorización, definir el monto de contribución por cada predio y construir las obras.
Apoyo	Atención al usuario	Administrar, apoyar y velar por los procesos relacionados con la atención al cliente a nivel interno y externo, a través de la formulación de estrategias y la implementación de una cultura del servicio empleando para ellos todas las herramientas tecnológicos y los canales de comunicación que posea la entidad, con orientación hacia la calidad, el mejoramiento continuo y el aumento de la satisfacción.
Apoyo	Comunicación Pública e información	Informar y comunicar las políticas, acciones y avances de los proyectos que emprende la Entidad de manera veraz y oportuna, con el fin de garantizar la transparencia de los procesos y la toma de decisiones para mantener una constante interacción con los clientes internos y externos de la Entidad.
Apoyo	Gestión Jurídica	Estudio y análisis a los conceptos y lineamientos normativos, con el fin de que las acciones de la entidad se ajusten a la normatividad vigente, se propenda por la prevención del daño jurídico, se desarrollen los procesos judiciales y se efectué la defensa de los intereses patrimoniales y judiciales de la entidad.
Apoyo	Gestión Financiera	Administrar los recursos financieros, mediante el seguimiento al recaudo, ejecución presupuestal y registro de las operaciones contables, como también la gestión de pagos y facturación, con el fin de garantizar la sostenibilidad financiera y brindar información confiable para la toma de decisiones.
Apoyo	Gestión Humana	Diseñar, definir, coordinar y verificar políticas, planes, programas y proyectos relacionados con el proceso de Gestión del Talento Humano de la Entidad, para el fortalecimiento de las capacidades técnicas y competencias comportamentales de los funcionarios de INVAMA.
Apoyo	Gestión Documental	Establecer las directrices, estructura y presentación para la elaboración, administración y control
Apoyo	Gestión de las Tecnología de la información	Asesorar, implementar, administrar, soportar las tecnologías de la información y comunicaciones de la entidad garantizando la continuidad, disponibilidad y seguridad de la infraestructura tecnológica.
Apoyo	Administración de bienes y servicios	Gestionar el Plan Anual de Adquisiciones que garantice todas las necesidades de compras de la entidad, administrar los inventarios y bienes

		patrimoniales de la entidad, garantizando su funcionamiento y protección; además de mantener en condiciones óptimas el parque automotor del Instituto
Evaluación y Control	Control de Gestión	Establecer la planeación y ejecución de métodos de evaluación, control y mejora continua de los procesos que integran el Modelo Integrado de Planeación y Gestión MIPG, con el fin de asegurar el cumplimiento de las metas, los objetivos institucionales y los principios de la entidad.

Fuente: INVAMA

7.2 Necesidades y Expectativas de los Interesados

La identificación de las partes interesadas *(Tabla 2)*, es una parte muy importante; debido a que se definen los requisitos tácitos, legales, reglamentarios y contractuales de la organización, empleados, clientes, proveedores, gobierno, comunidad, entre otros, que pueden influir directamente en la seguridad y privacidad de la información de la Entidad o que pueden verse afectados en caso de que estas se vean comprometidas. Así mismo, conocer las necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información de cada parte interesada.

Tabla 2. Necesidades y Expectativas frente a Seguridad y Privacidad de la Información

Parte Interesada	Descripción	Necesidades y Expectativas frente a Seguridad y Privacidad de la Información
Usuarios directos	Directivos	- Cumplir con los requisitos legales que le apliquen a la Entidad. - Realizar una adecuada gestión de riesgos. - Información oportuna, segura y confiable.
Usuarios directos	Funcionarios Servidores Públicos, Contratistas	- Contar con una infraestructura tecnológica segura, confiable y disponible. - Respuesta oportuna a requerimientos e incidentes. - Automatizar procesos de la Entidad. - Promover actividades de toma de conciencia y formación en temas de seguridad de la información. - Capacitar y socializar políticas, procedimientos y documentación del SGSI.
Entidades públicas – Gobierno	Autoridades del sector y entes del Estado	- Cumplimiento de los requisitos legales. - Garantizar la confidencialidad, disponibilidad e integridad de la información que maneja la Entidad. - Reportar los incidentes de seguridad ante el CSIRT. - Mantener canales de comunicación claros, disponibles y oportunos.

Entidades públicas – Gobierno	Entes de Control	- Articular con las entidades de control para evitar la violación del tratamiento de los datos personales. - Responder de forma oportuna a las comunicaciones requeridas. - Garantizar la seguridad, confidencialidad e integridad de la información.
Usuarios indirectos	Ciudadanía	- Servicios disponibles, seguros y confiables. - Protección de los datos personales del ciudadano. - Derecho al acceso de la información pública. - Contar con mecanismos de respuestas claras y oportunas a las PQRSD.
Terceros relacionados	Proveedores	- Confidencialidad en la información suministrada. - Pagos seguros y confiables
Terceros relacionados	Entidades Financieras	- Canales seguros para transferencia de información.

Fuente: Propia

7.3 Roles y Responsabilidades

Con el fin de poder realizar la labor de la manera más eficiente y de acuerdo a la "Guía de Roles y Responsabilidades del MinTIC" y a la aprobación de roles en acta 01 del 17-04-2023 por el Comité de Gestión y Desempeño Institucional, se presentan a continuación los roles y responsabilidades del SGSI.

Tabla 3. Roles y Responsabilidades

Rol	Descripción del Rol	Funciones	Funcionario Responsable
Alta Dirección	Responsable de revisar el Sistema de Gestión de Seguridad de la Información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continúa.	✓ 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.	Gerente y Líderes de Unidad

Responsable de TI	Responsable de planificar, organizar, coordinar, gestionar, controlar la estrategia de uso y apropiación de TI.	✓ 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. ✓ Identificar y reportar riesgos, eventos o incidentes de ciberseguridad a través de los canales definidos. ✓ Coordinar la administración, configuración de los recursos informáticos dentro de la plataforma tecnológica de seguridad. ✓ Planear y ejecutar el plan de mantenimiento y actualización de la infraestructura tecnológica y de telecomunicaciones de la entidad.	Profesional Universitario Sistemas
Responsable de Seguridad y Privacidad de la Información y Protección de Datos Personales **	Responsable de coordinar todas las actividades relacionadas con la gestión de la seguridad de la información.	✓ Fomentar la implementación de la Política de Gobierno Digital. ✓ Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información para la Entidad de conformidad con la regulación vigente. ✓ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad. ✓ Realizar la estimación, planificación y cronograma de la implementación del MSPI. ✓ Liderar la implementación y hacer seguimiento a las tareas y cronograma definido. ✓ Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI. ✓ Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de	Técnico Administrativo Sistemas

		información a desarrollar, actualizar o adquirir dentro de la entidad. ✓ Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. ✓ Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información. ✓ Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas. ✓ Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. ✓ Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad. ✓ Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información. ✓ Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atentes contra	

		la seguridad y privacidad de la información de acuerdo con la normativa vigente. ✓ Consolidar la información de Base de datos personales que maneja o tiene la entidad.	
Gestión del Talento Humano		✓ 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. ✓ Controlar y salvaguardar la información de datos personales del personal de planta de la entidad, en concordancia con la normatividad vigente. ✓ Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.	Profesional Universitario Gestión Humana
Área Jurídica		✓ Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. ✓ Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información. ✓ Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de	Líder Unidad Jurídica

		derechos de autor, confidencialidad y no divulgación de la información según sea el caso. ✓ Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información. ✓ Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.	
Área Comunicación y Prensa		✓ Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.	Profesional Universitario Comunicaciones
Comité de seguridad de la información o equivalente *(Comité Institucional de Gestión y Desempeño)	Responsable de la aprobación de las diversas directrices y normas asociadas a la seguridad de la información.	✓ Aprobar y hacer seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información. ✓ Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad. ✓ Aprobar acciones y mejores prácticas que en la implementación del MSPI. ✓ Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información. ✓ Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. ✓ Poner en conocimiento de la entidad, los documentos generados al interior del	Líderes de Unidad

		comité de seguridad de la información que impacten de manera transversal a la misma.	
Líderes de Proceso	Responsables de la información que se genera y se utiliza en las operaciones de su proceso.	✓ Asegurarse de que los activos estén inventariados. ✓ Asegurarse de la clasificación y adecuada protección de los activos. ✓ Dar cumplimiento a las restricciones establecidas a través de las diferentes políticas de control de acceso definidas. ✓ Asegurarse del adecuado manejo de los activos cuando este se elimina o destruye. ✓ Definir los usuarios que deben tener permisos de acceso a la información de acuerdo a sus funciones y competencias.	
Usuarios de la Información (funcionarios, Contratistas, Terceros)	Personas que utilizan la información y los activos tecnológicos en la Entidad para la normal ejecución de sus procesos.	✓ 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, lineamientos y procedimientos de seguridad y privacidad de la información definida y aprobada. ✓ Comunicar al responsable de Seguridad de la Información de las anomalías o incidentes de seguridad, así como de las situaciones sospechosas. ✓ Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos. ✓ Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.	
Auditores SGSI	Responsable de revisar el cumplimiento del SGSI	✓ Llevar a cabo auditorías internas a intervalos planificados con miras a proporcionar información acerca del estado actual del	

		Sistema de Gestión de Seguridad de la Información.	

Fuente: Propia

* Dado que la Entidad ya cuenta con un Comité de Gestión y Desempeño Institucional y teniendo presente que en dicho Comité tiene como una de las funciones “Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información”, no es necesario conformar un Comité de Seguridad y Privacidad de la Información.

** Así mismo se plantea que el responsable de Tratamiento de Datos Personales será la misma persona responsable de Seguridad y Privacidad de la Información en la Entidad.

7.4 Identificación de Activos de Información e Infraestructura Critica Cibernética

La Entidad cuenta con un inventario de activos de información **GT-SP-FO-02 Inventario de activos de información**, que incluye sistemas de información, bases de datos, infraestructura tecnológica y servicios tercerizados, los cuales se clasifican de acuerdo con su nivel de confidencialidad, integridad y disponibilidad.

7.5 Gestión de Riesgos de Seguridad y Privacidad

La gestión de riesgos se realiza conforme a una metodología alineada con ISO 27005 y el MSPI, permitiendo identificar, analizar, evaluar y tratar los riesgos que puedan afectar la información y los datos personales. El detalle del tratamiento de riesgos se desarrolla en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

7.6 Controles de Seguridad y Privacidad

La Entidad implementa controles de seguridad de tipo administrativo, técnico y físico, orientados a:

- Control de accesos
- Seguridad en operaciones
- Seguridad en comunicaciones
- Copias de seguridad y recuperación

- Gestión de incidentes
- Protección de datos personales

7.7 Privacidad y Protección de Datos Personales

La Entidad adopta las medidas necesarias para garantizar el tratamiento adecuado de los datos personales, conforme a la Ley 1581 de 2012, incluyendo políticas de tratamiento, avisos de privacidad, atención de derechos de los titulares y registro de bases de datos ante la SIC, de acuerdo al procedimiento establecido **GT-SP-PR-07 Protección de Datos Personales y Privacidad de la Información.**

7.8 Capacitación y Concientización

Se implementará un Plan Anual de Capacitación y Concientización en Seguridad y Privacidad de la Información dirigido a funcionarios y contratistas, con el fin de fortalecer la cultura de seguridad institucional.

8. EVALUACIÓN DEL DESEMPEÑO

8.1 Indicadores de Gestión del MSPI

La Entidad define y aplica indicadores de gestión que permiten medir el desempeño, la eficacia y el nivel de avance del Modelo de Seguridad y Privacidad de la Información (MSPI), en concordancia con el ciclo PHVA y los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

Los indicadores del MSPI deberán permitir:

- Medir el grado de implementación de controles de seguridad.
- Evaluar la gestión de riesgos de seguridad y privacidad.
- Verificar el cumplimiento de los planes y actividades definidas.
- Apoyar la toma de decisiones por parte de la Alta Dirección.

Indicadores:

- **Porcentaje de riesgos críticos tratados:** (Número de riesgos críticos con tratamiento implementado / Total de riesgos críticos identificados) x 100.
- **Porcentaje de activos de información clasificados:** (Activos clasificados / Total de activos inventariados) x 100.
- **Porcentaje de funcionarios y contratistas capacitados en seguridad y privacidad:** (Personas capacitadas / Total de personas vinculadas) x 100.
- Número de incidentes de seguridad reportados y gestionados. (Incidentes gestionados oportunamente / Total de incidentes) x 100.
- **Cumplimiento del cronograma del PSPI:** (Actividades ejecutadas / Actividades programadas) x 100.

Los indicadores serán medidos de forma trimestral y presentados al Comité de Gestión y Desempeño Institucional para la toma de decisiones.

8.2 Seguimiento, Análisis y Evaluación

El seguimiento al MSPI se realizará de manera periódica mediante la revisión de los indicadores definidos, los resultados del Plan de Tratamiento de Riesgos, la gestión de incidentes y los avances de los planes y proyectos asociados.

Los resultados del seguimiento serán documentados y comunicados al Comité de Planeación y Gestión Institucional y a la Alta Dirección, como insumo para la toma de decisiones y la mejora continua del sistema.

8.3 Auditoría Interna del MSPI

La Entidad realizará auditorías internas al MSPI con el fin de verificar el cumplimiento de los requisitos normativos, la correcta implementación de los controles de seguridad y la efectividad del Sistema de Gestión de Seguridad de la Información.

Las auditorías internas se desarrollarán conforme al plan anual de auditoría y generarán informes con hallazgos, observaciones y recomendaciones.

8.4 Revisión por la Dirección

La Alta Dirección realizará, como mínimo una vez por vigencia, la revisión del MSPI, considerando:

- Resultados de auditorías internas y externas.
- Estado de los riesgos de seguridad y privacidad.
- Cumplimiento de objetivos e indicadores.
- Incidentes de seguridad relevantes.
- Oportunidades de mejora.

Las conclusiones de la revisión por la dirección serán documentadas y servirán como base para la mejora continua del MSPI.

9. ESTRATEGIA DE SEGURIDAD DIGITAL

El INVAMA establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI **GT-SP-PR-01 Implementación y Gestión del SGSI**, así como de la guía de gestión de riesgos de seguridad de la información **GT-SP-MA-02 Manual de Administración de Riesgos de Seguridad de la Información** y del procedimiento de gestión de incidentes **GT-SP-PR-04 Gestión de Incidentes de Seguridad de la Información**.

Por tal motivo, el INVAMA define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

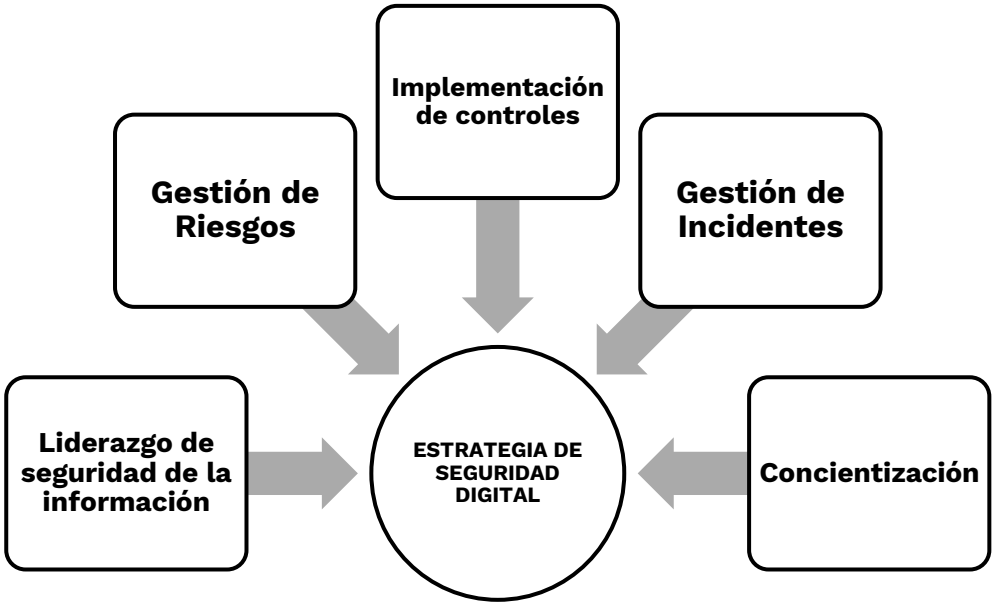

Figura 7. Estrategia de Seguridad Digital

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar:

Tabla 4. Estrategia de Seguridad Digital

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

9.1 Portafolio de Proyectos - Actividades

El Instituto de Valorización de Manizales – INVAMA -, ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) y para lograr su implementación y fortalecimiento ha diseñado un conjunto de planes orientados a avanzar en diferentes actividades para dar cumplimiento a las orientaciones del Ministerio de Tecnologías de Información y de las Comunicaciones.

En ese sentido, desde el INVAMA, se ha organizado un plan general para aportar en las acciones encaminadas a fortalecer el Modelo de Seguridad y Privacidad de la Información de la Entidad, como habilitador fundamental, para dar cumplimiento a lo estipulado en la Política de Gobierno Digital.

Para cada estrategia específica, el INVAMA define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Tabla 5. Portafolio de proyectos – actividades plan de seguridad y privacidad de información del INVAMA

Estrategia / Eje	Proyecto	Productos esperados	Responsable
Liderazgo de Seguridad de la Información	**Proyecto 1:** Actualizar la política general de seguridad y privacidad de la información.	Política de seguridad actualizada, formalizada e implementada.	Responsable de Seguridad y Privacidad de la Información
	Proyecto 2: Elaborar las políticas específicas de seguridad y privacidad de la información.	Política específicas formalizada e implementada.	Responsable de Seguridad y Privacidad de la Información
	Proyecto 3: Actualizar la política de tratamiento y protección de datos personales.	Política de tratamiento de datos actualizada, formalizada e implementada.	Responsable de Seguridad y Privacidad de la Información
	Proyecto 4: Actualizar la política de seguridad de la información del sitio web.	Política de seguridad de sitio web actualizada, formalizada e implementada.	Responsable de Seguridad y Privacidad de la Información
	Proyecto 5: Recolección y revisión de bases de datos personales ante la SIC.	Base de Datos personales actualizada ante el SIC.	Responsable de Seguridad y Privacidad de la Información
	Proyecto 6: Definir el plan de continuidad de negocio y recuperación de desastres.	Plan de continuidad de negocio y recuperación de desastres aprobado e implementado.	Responsable de Seguridad y Privacidad de la Información
	Proyecto 7: Seguimiento a los indicadores del SGSI.	Indicadores SGSI documentados, aprobados e implementados.	Responsable de Seguridad y Privacidad de la Información.
	Proyecto 19: Realizar el estudio y contratación para el servicio de Backup en la nube	Servicio adquirido y configurado	Responsable de TI
	Proyecto 20: Realizar el estudio y contratación para el servicio de Antivirus.	Servicio adquirido y configurado	Responsable de TI
	Proyecto 21: Realizar el estudio y contratación para el servicio de Firewall.	Servicio adquirido y configurado	Responsable de TI

Gestión de Riesgos	**Proyecto 8:** Identificar, valorar y clasificar los riesgos asociados a los activos de información.	Activos e Información	Responsable de Seguridad y Privacidad de la Información – Líderes de Proceso
	Proyecto 9: Definir planes de tratamiento de riesgos de seguridad.	Análisis de vulnerabildiades	Responsable de Seguridad y Privacidad de la Información – Responsable de TI
	Proyecto 22: Actualizar los activos de información.	Matriz de riesgos de seguridad digital.	Responsable de Seguridad y Privacidad de la Información – Líderes de Proceso
	Proyecto 23: Identificar amenazas y vulnerabilidades para cada activo crítico	Plan de tratamiento de riesgos aprobados por la alta dirección.	Responsable de Seguridad y Privacidad de la Información – Alta Dirección
Implementación de controles	**Proyecto 10:** Implementar Controles Organizacionales	Controles implementados	Responsable de Seguridad y Privacidad de la Información – Responsable de TI
	Proyecto 11: Implementar Controles de Personas	Controles implementados	
	Proyecto 12: Implementar Controles Físicos	Controles implementados	
	Proyecto 13: Implementar Controles Tecnológicos	Controles implementados	
	Proyecto 14: Creación de procedimientos de la entidad en lo relacionado a seguridad de la información.	Procedimientos documentados, socializados y aprobados.	
	Proyecto 24: Implementar controles que mitiguen las vulnerabilidades de los activos críticos.	Controles implementados	
Gestión de incidentes	**Proyecto 16:** Capacitar al personal en la gestión de incidentes de seguridad de la información.	Procedimiento de gestión de incidentes de seguridad formalizado.	Responsable de Seguridad y Privacidad de la Información

		Sesiones de capacitación desarrolladas.	Responsable de Seguridad y Privacidad de la Información
Concientización	**Proyecto 17:** Establecer el plan de comunicación, capacitación, sensibilización y concientización para la Entidad. **Proyecto 18:** Realizar jornadas de comunicación, capacitación sensibilización y concientización para todo el personal de la Entidad.	Plan de comunicación, capacitación, sensibilización y concientización. Evidencias de las actividades desarrolladas.	Responsable de Seguridad y Privacidad de la Información – Gestión Talento Humano Responsable de Seguridad y Privacidad de la Información – Área Comunicación

9.2 Cronograma de Actividades / Proyectos

Tabla 6. Cronograma de Actividades / Proyectos

	2025			
FASE	**TRIMESTRE 1**	**TRIMESTRE 2**	**TRIMESTRE 3**	**TRIMESTRE 4**
Planificación y organización	P1. Actualizar política general de seguridad y privacidad de la información. P3. Actualizar la política de tratamiento y protección de datos personales. P4. Actualizar la política de seguridad de la información del sitio web. P5. Recolección y revisión de bases de datos personales ante el SIC. P17. Establecer el plan de comunicación, capacitación, sensibilización y concientización para la Entidad. P21: Realizar el estudio y contratación para el servicio de Firewall.	P18. Realizar jornadas de comunicación, capacitación sensibilización y concientización para todo el personal de la Entidad.	P18. Realizar jornadas de comunicación, capacitación sensibilización y concientización para todo el personal de la Entidad.	P19. Realizar el estudio y contratación para el servicio de Backup en la nube P20. Realizar el estudio y contratación para el servicio de Antivirus P18. Realizar jornadas de comunicación, capacitación sensibilización y concientización para todo el personal de la Entidad.

Desarrollo de políticas y procedimientos	P2. Elaborar las políticas específicas de seguridad y privacidad de la información. P6. Definir el plan de continuidad de negocio y recuperación de desastres – DRP. P16. Capacitar al personal en la gestión de incidentes de seguridad de la información.	P14. Creación de procedimientos de la entidad en lo relacionado a seguridad de la información.		
Análisis de riesgos, selección e implementación de controles	P22. Actualizar los activos de información. P23. Identificar amenazas y vulnerabilidades para cada activo crítico.	P8. Identificar, valorar y clasificar los riesgos asociados a los activos de información. P9. Definir planes de tratamiento de riesgos de seguridad. P10. Implementar Controles Organizacionales	P11. Implementar Controles de Personas P24. Implementar Controles que mitiguen las vulnerabilidades de los activos críticos.	P12. Implementar Controles de Físicos. P13. Implementar Controles de Tecnológicos.
Evaluación de desempeño y mejora continua	P7. Seguimiento a los indicadores del SGSI	P7. Seguimiento a los indicadores del SGSI	P7. Seguimiento a los indicadores del SGSI	P7. Seguimiento a los indicadores del SGSI

Fuente: Propia

Nota: Al finalizar cada vigencia, El INVAMA, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

10 APROBACIÓN Y VIGENCIA

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el comité de gestión y desempeño institucional, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

El Plan de Seguridad y Privacidad de la Información se adoptan mediante acto administrativo y tendrán vigencia anual.

El PSPI deberá ser revisado y actualizado cuando se presenten cambios normativos, organizacionales o tecnológicos relevantes, o como resultado de auditorías, incidentes de seguridad o revisiones por la dirección.