Plan de Seguridad y Privacidad de la Información

2024

Instituto de Valorización de Manizales

INVAMA

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Manizales, Enero de 2024

Versión 4

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

CONTENIDO

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

INDICE DE TABLAS

Calle 3C#22-92 Barrio Alcázares Manizales
Tel:(6)8891030 www.invama.gov.co

INDICE DE FIGURAS

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

INTRODUCCION

La Estrategia de Gobierno Digital, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

El INVAMA, reconoce la importancia y ha identificado la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones dado que en la gestión de los procesos estratégicos, misionales y de apoyo, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa para la Entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de Gestión y Seguridad de la Información, siguiendo los lineamientos del MSPI de la Estrategia de Gobierno Digital, a su vez reglamentado a través del Decreto 1008 de 2018, Decreto 1078 de 2015 y el Decreto 2573 de 2014 y el CONPES 3854 de 2016, por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, el

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

SGSI del INVAMA adoptará una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

Así mismo, el SGSI del INVAMA definirá políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoria y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

Lo anterior se complementa con los programas de formación y transferencia de conocimiento en seguridad de la información y las campañas de sensibilización que se liderarán al interior de la entidad. Así pues, la entidad expone a través de este manual el modelo del SGSI adoptado por la entidad de acuerdo al ciclo PHVA (planear, hacer, verificar y actuar), con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada.

Dicho plan establecerá el contexto, las políticas, los objetivos, el alcance, los procedimientos, las metodologías, los roles, las responsabilidades y las autoridades del SGSI; de acuerdo con los requisitos legales, los contractuales y los normativos, que le aplican a la entidad, en el marco de seguridad de la información. Para tal fin, la entidad ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como ISO 27002:2015, ISO 27005:2009, el modelo nacional de riesgos de seguridad digital y las guías definidas por el MinTIC para la implementación del MSPI; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

1. JUSTIFICACIÓN

El Instituto de Valorización de Manizales – INVAMA - siendo una entidad pública, debe cumplir con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y a través de este plan se busca determinar cómo la entidad puede asegurar de forma efectiva la información generada y utilizada por los procesos misionales del negocio (Contribución de Valorización y Alumbrado Público). Sumado a la magnitud que representa dar el cumplimiento al componente de Seguridad de la Información de la Estrategia de Gobierno Digital, el cual se va a llevar a cabo por medio del Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) y brindará los procedimientos y lineamientos necesarios para identificar y evaluar los riesgos, las amenazas, las vulnerabilidades de los activos de información e implantar los controles necesarios que ayudaran a salvaguardar los activos de información, mantener y mejorar continuamente el SGSI, alienándolos a los objetivos estratégicos de la organización; con el objetivo de forjar, promover y extender una cultura de seguridad en todos los niveles de la organización y de este modo, gestionar de manera apropiada la seguridad de su información.

También es significativo fomentar la importancia del SGSI que exista un compromiso por parte de todas áreas de la entidad, las cuales deben formar parte activa del proceso, así como también es importante determinar los recursos económicos, físicos y humanos que posea la entidad, ya que dependiendo de éstos determinará el tratamiento de los riesgos y se asumirán compromisos con el proceso basado en la mejora continua.

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

2. OBJETIVO

Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad según el modelo del Sistema de Gestión de Seguridad de la Información – SGSI-, adoptado por el Instituto de Valorización de Manizales – INVAMA -; este documento expone las prioridades de implementación de los controles en relación a seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (Planear, Hacer, Verificar, Actuar)

2.1 OBJETIVOS ESPECÍFICOS

- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI -, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Administrar los eventos de seguridad de la información del INVAMA.
- Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica acorde con la declaración de aplicabilidad aprobada.
- Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
- Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas, pasantes, judicantes).
- Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

3. ALCANCE

EL SGSI es aplicable a los activos de información de todos los procesos del INVAMA, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad avalada por el Comité Institucional de Gestión y Desempeño.

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. De igual modo, 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 23 de 1982:** Derechos de Autor. Reglamenta todas las generalidades sobre las normas que protegen los derechos de autor para cualquier obra científica, literaria u artística.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.
- **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 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6) 8891030 · www.invama.gov.co

organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

- **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 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.
- **Decreto 235 de 2010.** Se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
- **Ley 1453 de 2011.** Seguridad ciudadana. Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
- **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.
- **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.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

- **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.
- **NTC ISO 27001: 2013.** Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
- **NTC ISO 27002: 2013.** Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
- **Ley 1712 de 2014**. **Ley de transparencia y del derecho de acceso a la información pública** Nacional 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 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- **Decreto 1499 de 2017**. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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 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.
- **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.
- **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.
- **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
- **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.
- **Directiva Presidencial 03 de 2021**. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- **Resolución 00500 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 088 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

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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.
- **Decreto 338 de 2022**. Adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.
- **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.

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).

- **Amenazas:** 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)

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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

- **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

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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).

- **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).

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

- **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).

- **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.

- **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.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

- **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. (ArCert).

- **Registro Nacional de Bases de Datos:** 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).

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

- **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).

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN –MSPI

El modelo de seguridad y privacidad de MSPI de la estrategia de gobierno digital explora los siguientes ciclos de acción, que incluyen cinco (5) fases las cuales son: Diagnostico, planificación, implementación, gestión y mejoramiento continuo; para permitir que las entidades gestionen adecuadamente la seguridad y la privacidad de sus activos de información.

Figura 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información.

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

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

6.1 FASE DE DIAGNÓSTICO

Esta etapa de DIAGNÓSTICO según ISO 27001:2022 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 2. Etapas previas a la implementación

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

6.1.1 Estado actual de la entidad e Identificación del nivel de madurez

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.

El diligenciamiento de la Herramienta Instructivo de Evaluación MPSI, permitió obtener una calificación calculada para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control que se establecen, todo esto referenciado desde las hojas nombradas como "ADMINISTRATIVAS y TÉCNICAS" dentro de la Herramienta Instrumento MSPI de acuerdo a Instrumento Instructivo Evaluación MPSI. El resultado obtenido para la evaluación del estado actual nos refleja los controles y su efectividad según la Normatividad NTC/ISO 27001 del 2013 (Figura 3) y lo planteado dentro del desarrollo del modelo de seguridad y privacidad de la información que ha establecido el MinTIC para las entidades públicas de orden territorial, así como el avance del ciclo PHVA (Planear-Hacer-Verificar-Actuar).

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	18	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	19	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	18	100	INICIAL
A.9	CONTROL DE ACCESO	57	100	EFECTIVO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	45	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	51	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	15	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	26	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	10	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4	100	INICIAL
A.18	CUMPLIMIENTO	31	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**28**	**100**	REPETIBLE

Figura 3. Evaluación de efectividad de Controles - ISO 27001:2013

Fuente: Instrumento de Evaluación MSPI – Portada

De acuerdo con el análisis y los resultados obtenidos *(figura 3)*, la calificación promediada de los controles dentro de la entidad fue de **28**, lo cual evidencia que la entidad se encuentra en un proceso **INICIAL** de implementación de medidas para la seguridad y privacidad de la información.

Sin embargo, se precisan los **10** dominios que deben ser incluidos entre las acciones de la actual vigencia para su fortalecimiento (Figura 4):

- A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- A.7 SEGURIDAD DE LOS RECURSOS HUMANOS
- A.8. GESTIÓN DE LOS ACTIVOS
- A.10 CRIPTOGRAFÍA
- A.13 SEGURIDAD DE LAS COMUNICACIONES
- A.14, ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
- A.15 RELACIÓN CON LOS PROVEEDORES
- A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
- A.20 CUMPLIMIENTO.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Figura 4. Brecha Anexo A ISO-27001:2013

Fuente: Instrumento de Evaluación MSPI – Portada

6.2. FASE DE PLANIFICACIÓN

Esta fase de PLANIFICACIÓN que cumple con ISO 27001:2022 en el Capítulo 5 - Liderazgo, define las responsabilidades y obligaciones de la alta dirección en relación con el sistema de gestión de seguridad de la información, incluida la necesidad de que la alta dirección prepare una política de seguridad de la información adecuada a la alcaldía, que asegura la distribución de los recursos del SGSI, la distribución, comunicación de responsabilidades y roles importantes desde el punto de vista de la seguridad de la información.
En el capítulo 6 – Planificación, se establecen los requerimientos para la valoración y tratamiento de riesgos de seguridad, la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

En el Capítulo 7 – Soporte, se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información.

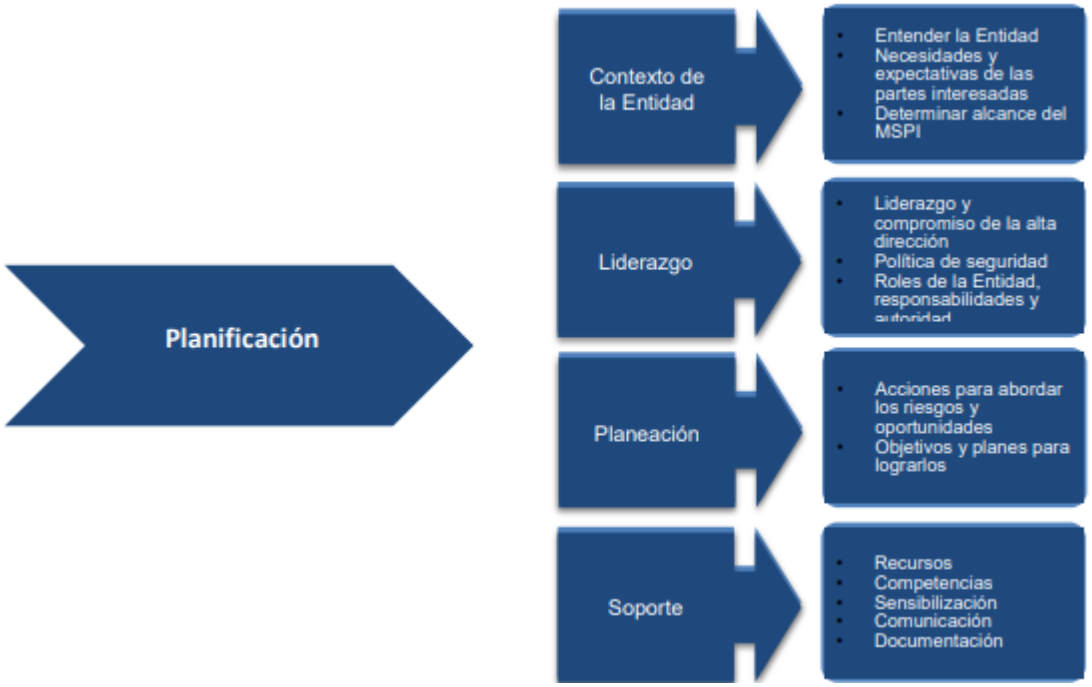

Figura 5. Fase de Planificación

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

6.2.1. Contexto de la Entidad

El propósito es conocer en detalle las características de la Entidad y su entorno, que permitan implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas del INVAMA, determinando los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la Entidad.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6.2.1.1. Conocimiento 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.** Prestar el servicio de Alumbrado Público y desarrollar proyectos por el Sistema de Contribución de Valorización con calidad y oportunidad, basados en la sostenibilidad y trabajo en equipo, generando seguridad y progreso a la comunidad.

B. **Visión de la Entidad.** Para el 2023, prestaremos el servicio de Alumbrado Público, enfocados en nuevas tecnologías y el uso racional de energía y la ejecución de proyectos por el Sistema de Contribución de Valorización, enfocados al desarrollo económico y social de la comunidad.

C. **Estructura Organizacional.** Tal como se puede apreciar en la *Figura 3* se presenta la estructura organizacional del INVAMA de acuerdo al acuerdo número 004 del 28 de octubre de 2018.

Calle 3C#22-92 Barrio Alcázares Manizales
Tel:(6)8891030 www.invama.gov.co

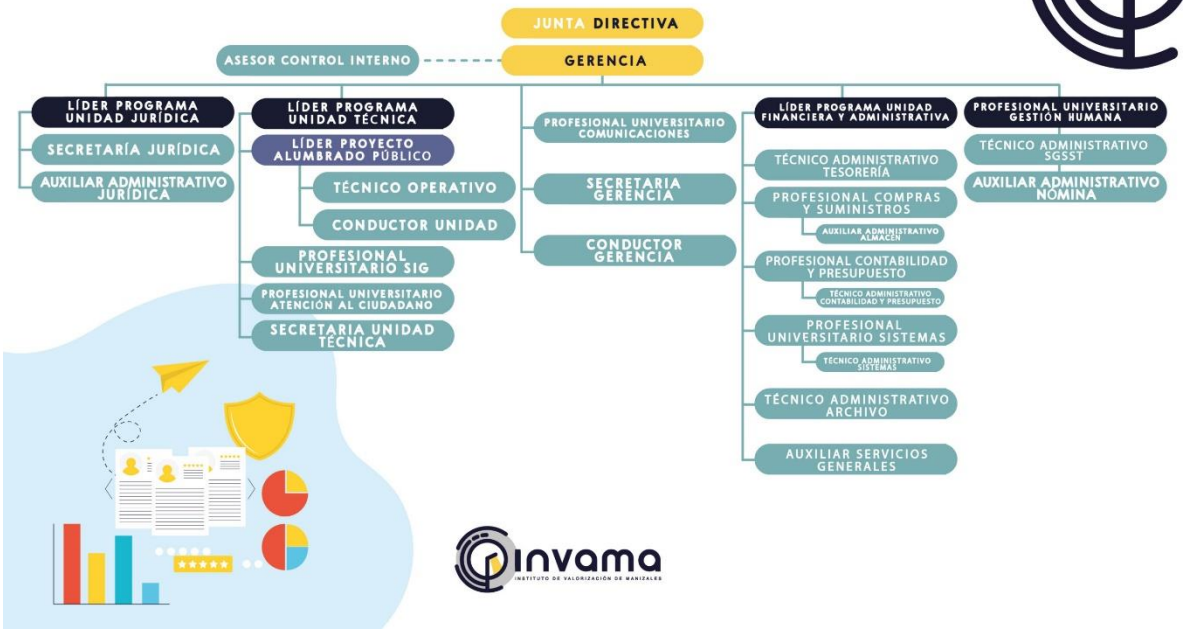

Figura 6. Estructura Organizacional de INVAMA

Fuente: INVAMA

D. **Mapa de Procesos.** INVAMA se encuentra estructurada por procesos, tal como se puede apreciar en la *figura 4* se definen en procesos estratégicos, misionales, apoyo y evaluación y control, en la *tabla* 1 podemos apreciar la descripción de cada proceso.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Figura 7. Mapa de Procesos de INVAMA

Fuente: INVAMA

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

		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.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		MIPG, con el fin de asegurar el cumplimiento de las metas, los objetivos institucionales y los principios de la entidad.

Fuente: INVAMA

6.2.1.2. Necesidades y Expectativas de las Partes Interesadas Frente a Seguridad y Privacidad de la Información.

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.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		- 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.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		- 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

6.2.2.3. Determinación del alcance del Sistema de Gestión de Seguridad de la Información.

Para determinar el alcance del SGSI de Invama, se realizó una revisión a los procesos de la Entidad con el fin de determinar: ¿Cuál es la información más crítica? y ¿Qué servicios deben estar disponibles para los usuarios? En respuesta a las preguntas se aplicará el MSPI para sus dos procesos misionales relacionados con Proyectos de Valorización y Alumbrado Público.

6.2.2. Liderazgo

6.2.2.1. Liderazgo y compromiso de la alta dirección

En el acto administrativo 207 del 02-08-2023 que soporta y conforma el Comité de Gestión y Desempeño MIPG, señala las funciones de seguridad y privacidad de la información de la Entidad, Artículo tercero, numeral 6 así: “Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información”; por tal motivo y por ser una Entidad pequeña en planta de personal administrativa, las funciones establecidas para el Comité de Seguridad y Privacidad de la

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

Información, harán parte del Comité Institucional de Planeación y Gestión MIPG.

6.2.2.2. Política de seguridad

Teniendo en cuenta la misión, el contexto de la Entidad y el alcance definido del SGSI para el INVAMA, se elaboraron las diferentes políticas de seguridad de la información para la Entidad, basado en la "Guía de elaboración de la política general de seguridad y privacidad de la información y en las herramientas suministradas por Gobierno Digital.

A. Política General de Seguridad y Privacidad de la Información.

La Política General de Seguridad y Privacidad de la información de INVAMA, https://invama.gov.co/wp-content/uploads/2023/09/Politica-General-de-Seguridad-y-privacidad-de-la-Informacion-INVAMA-2023.pdf corresponde a la declaración general que representa la posición de la Entidad con respecto a la protección de los activos de información que soportan los procesos de la organización y apoyan la implementación del SGSI, así como la asignación de roles y responsabilidades generales para la gestión de la seguridad y privacidad de la información del INVAMA.

B. Políticas Específicas de Seguridad y Privacidad de la Información.

En el documento "Políticas Específicas de Seguridad y Privacidad de la Información", se agrupan las políticas específicas con el objetivo de hacer una implementación transversal de Seguridad y Privacidad de la Información en el INVAMA y se convierten en la base de implementación, mantenimiento y mejora de los controles en la Entidad basados en 14 políticas:

- Políticas de Dispositivos Móviles
- Políticas de Teletrabajo
- Políticas de Seguridad de los Recursos humanos
- Políticas de Gestión de activos
- Políticas de Control de acceso

- Políticas de Seguridad física y del entorno
- Políticas de Seguridad en las operaciones
- Políticas de Seguridad de las comunicaciones
- Políticas de Controles criptográficos
- Políticas de Adquisición, desarrollo y mantenimiento de sistemas
- Políticas de Relaciones con los proveedores
- Políticas de Gestión de incidentes de seguridad de la información
- Políticas de Seguridad de la Información en la Continuidad del Negocio
- Políticas de Cumplimiento

C. Política de Tratamiento y Protección de Datos Personales

La Política para el Tratamiento y Protección de datos Personales para el INVAMA http://https//invama.gov.co/wp-content/uploads/2021/02/Pol%C3%ADtica-de-Tratamiento-y-Protecci%C3%B3n-de-Datos-Personales.pdf proporciona los lineamientos necesarios para el cumplimiento de las obligaciones legales en materia de protección de datos personales, cuya aplicación es de carácter obligatorio para todas las personas naturales o jurídicas que hagan tratamiento de los datos personales registrados en las bases de datos del INVAMA.

D. Política de Seguridad de la Información del Sitio Web

La Política de Seguridad de la Información del Sitio Web de INVAMA, http://https//invama.gov.co/wp-content/uploads/2021/02/Pol%C3%ADticas-de-seguridad-de-la-informaci%C3%B3n-del-sitio-web-Condiciones-de-uso-1.pdf establece la información suministrada por los usuarios del sitio web para la ejecución de los trámites en línea, las políticas se entenderán aceptadas por el usuario al ingresar al sitio web.

6.2.2.3. Roles de la Entidad Responsabilidad y Autoridades

Con el fin de poder realizar la labor de la manera más eficiente y teniendo en cuenta el número de empleados de la Entidad y de acuerdo a la “Guía de Roles y Responsabilidades del MinTIC” y la propuesta metodológica para la implementación de un SGSI, se sugiere:

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

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	Profesional Universitario Sistemas

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		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.	
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	Técnico Administrativo Sistemas

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		de seguridad que deberán cumplir los sistemas de 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	

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		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.	Profesional Universitario Gestión Humana

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		✓ 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.	
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 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	Líder Unidad Jurídica

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		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	Líderes de Unidad

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		esta revisión definir las acciones pertinentes. ✓ Poner en conocimiento de la entidad, los documentos generados al interior del 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	

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		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.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6.2.3. Planeación

6.2.3.1. Acciones para abordar los riesgos y oportunidades

De acuerdo a la *Guía de Clasificación de Activos de Información* establecida por el MinTic y a la propuesta de clasificación de activos del SGSI se realizó el inventario de activos tecnológicos por capas y nivel de dependencia para los procesos definidos en el alcance, para lo cual se recolectaron los siguientes datos:

Tabla 4. Identificación del activo de información

	Campo	Descripción
IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN (LEY 594 DE 2000 - LEY 1712 DE 2014- DECRETO 103 DE 2015 - DECRETO	N° Activo	Número consecutivo único que identifica al activo en el inventario.
	Tipo de Proceso	Tipo de Proceso de la Entidad al que pertenece el activo de información. (Estratégico, Misional, Apoyo, Evaluación)
	Proceso de Negocio	Nombre del Proceso de la Entidad al que pertenece el activo de información.
	Código Documento MIPG	Relacionar el código con el que se encuentra registrado en los documentos de calidad MIPG.
	Identificador	Consecutivo del activo de información. Identificador Único.
	Tipo / Capa	Capa por dependencia a la que pertenece el activo de información. *Ver Figura 8 Capas de Activo de Información.*

Calle 3C#22-92 Barrio Alcázares Manizales
Tel:(6)8891030 www.invama.gov.co

	Ubicación	Describe la ubicación tanto física como electrónica del activo de información.
	Nombre Activo	Nombre de identificación del activo.
	Descripción	Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
	Serie Documental	Serie documental del Activo de Información. Aplica cuando el activo es de tipo Datos/Información/conocimiento
	Nombre del responsable de la producción de la información (Propietario del activo)	Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
	Nombre del responsable de la información (Custodio del activo)	Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia,

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

		el custodio generalmente se define donde reposa el activo original).
	Usuarios	Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.
	Fecha de ingreso del activo al inventario	Fecha de ingreso del activo de información en el inventario.
	Soporte de registro	De acuerdo con el Decreto 2609 de 2012: Físico (análogo) Digital (electrónico) Este campo se diligencia si el Tipo de activo es “Datos/Información/Conocimiento", para el resto de tipos de activos se debe seleccionar N/A.
	Medio de conservación	De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger. (Documentos Archivo físicos, Documentos Archivo Electrónicos, Sistemas de Información, Sistema Administración de Documentos, Sistema de Mensajería Electrónica, Portales, Intranet, Extranet, Sistemas de Bases de Datos, Discos Duros, Servidores, discos o medios portables, cintas o medios

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		de video y audio (análogo o digital), Cintas y medios de soporte (backup y contingencia), Uso de tecnologías en la nube)
	Formato	Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como : Hoja de cálculo, imagen, audio, video, documento de texto, Bases de datos, página web, papel, PDF, etc.
	Idioma	Establece el idioma, lengua o dialecto en que se encuentra la información.
	Servicio de TI	Servicio de Tecnología de Información a la que pertenece el activo (Servicio Correo Electrónico Institucional, Servicio Internet, Servicio Publicación en página web, Servicio de Sistemas de Información, Servicio de Video Conferencia, Servicio de Soporte y mantenimiento a usuarios internos, Servicio de Formulación y dirección de proyectos de TI, Servicio de Infraestructura y plataforma TIC, Servicio Sede Electrónica o Portal Web, Servicio de Backup automatizado, Servicio de Procesamiento de Información, Servicio de Redes y Comunicaciones)
	Marca	Marca del activo, cuando el tipo de activo es Hardware.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	Serial	Serial del activo, cuando el tipo de activo es Hardware.
	Capacidad	Capacidad del activo, cuando el tipo de activo es Hardware.
ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (DECRETO 103 DE 2015)	Índice de Información Clasificada y Reservada	Corresponde a los criterios de clasificación de la información, con el fin de identificar qué activos deben ser tratados de manera prioritaria. *Ver Figura 9 Índice de Información Clasificada y Reservada*
	Información publicada	Publicada: Si la información es pública y se puede consultar en un sitio web (interno o externo) o un sistema de información del Estado. Publicada (Interno - Intranet) Publicada (Externo - Internet) No Publicada: Si la información se encuentra en la Entidad pero no se encuentra en un sistema de información o sitio web
	Lugar de consulta o ubicación	Indica la URL, sitio web o sistema de información donde puede ser consultada la información si esta se encuentra pública, el lugar de consulta si no está publicada o ubicación física.
	Objeto legítimo de la excepción	La identificación de la excepción que, dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cobija la calificación de información reservada o

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6) 8891030 · www.invama.gov.co

		clasificada. Si la respuesta es NO se debe marcar no aplica (N/A) en los demás campos sobe el índice de información clasificada y reservada.
	Fundamento constitucional o legal	Indica el fundamento constitucional o legal que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la ampara.
	Fundamento jurídico de la excepción	Indica la norma jurídica que sirve como fundamento jurídico para la clasificación o reserva de la información.
	Excepción total o parcial	Según sea integral o parcial la calificación, las partes o secciones clasificadas o reservadas. Indicar si la totalidad del documento es clasificado o reservado o si solo una parte corresponde a esta calificación.
DATOS PERSONALES (LEY 1581 DE 2012)	¿Contiene datos personales?	¿El activo de información contiene datos personales? SI – NO
	Tipos de datos personales	Si cuenta con datos personales seleccione el tipo, en caso contrario seleccione N/A: Dato personal público: Toda información personal que es de conocimiento libre y abierto para el público en general. Ejemplo: Número de identificación apellidos. Dato personal privado: Toda información personal que tiene un conocimiento restringido, y en principio privado

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

		para el público en general. Ejemplo: (Fotografías, videos, datos relacionados con su estilo de vida, contenido correos electrónicos, contraseñas) Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector y grupo de personas. Ejemplo: (datos financieros y crediticios, dirección, teléfono, correo electrónico, datos socioeconómicos, datos relacionados con la actividad económica, historia laboral, nivel académico, antecedentes judiciales y disciplinarios, datos de información tributaria, datos socioeconómicos, correo personal, teléfono, fecha de nacimiento, edad). Dato Sensible: Protección reforzada. (Datos biométricos, datos de la descripción morfológica de la persona, datos relacionados con la salud, datos de preferencia de identidad, origen étnico, racial, población en condición vulnerable, datos personas en situación de discapacidad, datos con relación a pertenencia de sindicatos, organizaciones sociales, religiosas, políticas) Dato Abierto: Los datos abiertos pueden crearse y/o manipularse con cualquier software libre, aumentando

Calle 3C#22-92 Barrio Alcázares Manizales
Tel:(6)8891030 www.invama.gov.co

		así la reutilización de datos, este tipo de formatos son por ejemplo archivos .CSV, .TMX, .ODF, JSON.
	Clasificación Datos Personales	(Identidad, Trabajo, Patrimonio, Educación, Ideología, Físico, Salud, Intimidad)
	Existe la autorización para el tratamiento de los datos personales	Seleccionar si se cuenta o no con la autorización de la recolección y tratamiento
	¿Existe Transferencia Internacional de Datos Personales?	Seleccionar si existe transferencia de datos personales a nivel internacional.
CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)	Clasificación	Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.
	Confidencialidad	La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad. (Información Pública Reservada, Información Pública Clasificada, Información Pública, No Clasificada) de acuerdo a ley

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

		1712 del 2014. *Ver figura 10 Clasificación de la Confidencialidad.*
	Integridad	La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. (Alta, Media, Baja, No Clasificada). *Ver figura 11 Clasificación de la Integridad.*
	Disponibilidad	La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. (Alta, Media, Baja, No Clasificada). *Ver figura 12 Clasificación de la Disponibilidad*
	Criticidad	Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información. (Alta, Media, Baja). *Ver figura 13 Niveles de Clasificación de la Criticidad*
	Fecha Salida del Activo	Fecha de exclusión del activo de información del inventario.

Calle 3C#22-92 Barrio Alcázares Manizales
Tel:(6)8891030 www.invama.gov.co

Capas Tecnologias Información y Comunicaciones		Descripción
1	Procesos de Negocio	Los procesos de negocio son todas aquellas actividades desarrolladas por la organización para cumplir con sus objetivos. Tradicionalmente estas se encuentran asociadas en diferentes categorías tales como: procedimientos, los cuales en su conjunto conforman un proceso, y a su vez en su conjunto, se denominan macro procesos. Todas las organizaciones cuentan por lo general con un mapa de procesos, agrupados en estratégicos, misionales y de apoyo (o términos similares) los cuales reflejan la forma como opera la organización y el nivel de interrelación existente entre cada uno de ellos
2	Servicios de TI	de acuerdo a la definición planteada por ITIL, un servicio de TI es un medio por el cual se entregar valor a los clientes (usuarios) facilitándoles un resultado deseado sin la necesidad de que estos asuman los costos y riesgos específicos. Los servicios se construyen a partir de la combinación de la infraestructura tecnológica y los procesos de gestión y operación de TI. Algunos ejemplos de servicios son: correo electrónico, servicio de backups, servicio de procesamiento de nómina, servicio de soporte y mantenimiento, servicio de capacitación.
3	Datos/Información/Conocimiento	son los recursos más valiosos para la organización y los que en definitiva requieren mayor nivel de protección.
4	Sistemas de Información Transaccionales	son todos aquellos sistemas de información que utiliza la organización para automatizar sus procesos de negocio. Algunos ejemplos son: ERP (Enterprise Resource Planning), CRM (Customer Relation Management), sistemas de información de nómina, sistemas de información de ventas.
5	Sistemas de Información Soporte	son todas aquellas herramientas de software que apoyan el negocio y la función de tecnologías de información para cumplir diferentes funciones operacionales, y se diferencian de los sistemas de información transaccionales, en que estas herramientas no soportan un proceso de negocio en especial. Dentro de esta categoría podemos encontrar: herramientas ofimáticas, software antivirus, compiladores para desarrollo de software, herramientas RAD (Rapid Application Developer), software utilitario para apoyar diferentes funciones de tecnologías de información.
6	Motores de Bases de Datos	equivale a lo que en el mercado se conoce como sistemas gestores de bases de datos (SGBD), los cuales permiten añadir, borrar, modificar, almacenar y analizar los datos que tiene una organización y que son gestionados tradicionalmente a través de sistemas de información. Dentro de los principales motores de bases de datos se encuentran: Oracle, SQL Server, Postgresql, Mysql.
7	Sistemas Operativos	es el programa que se encarga de administrar los servicios de hardware de un computador personal, de un servidor o de cualquier dispositivo que requiere de un interfaz entre los recursos de hardware y las diferentes funcionalidades de uno o varios sistemas de información. Dentro de esta categoría existen diferentes tipologías de sistemas operativos, desde sistemas operativos para computadores o dispositivos personales de un solo usuario y monotarea, hasta sistemas operativos para servidores, que atienden diferentes tareas y diferentes usuarios. Algunos ejemplos de sistemas operativos: Sistemas operativos Windows (en sus diferentes versiones), Android, OS2 de IBM, Unix, Linux.
8	Pcs de Escritorio/Impresoras/Portatiles/Tablet	en el caso de los computadores personales (PC's) son los dispositivos que tradicionalmente tiene cualquier usuario en su escritorio y a través de los cuales pueden acceder a los diferentes sistemas de información de la organización; en el caso de las impresoras, son todos aquellos dispositivos a través de los cuales se puede llevar a papel la información contenida en medios virtuales.
9	Servidores (Físicos, Virtuales y en la nube)	Los servidores son computadores dotados de ciertas características especiales (mayor capacidad de procesamiento, multitarea, mayores capacidades de almacenamiento, mayor capacidad en memoria) que se encuentran al servicio de otros dispositivos, y tradicionalmente son dedicados a tareas especializadas, para lo cual toman nombres de acuerdo a la tarea especializada asignada: Servidor de aplicaciones, servidor de archivos, servidor de correo, servidor de impresoras, servidor de base de datos. Dentro de esta categoría podemos encontrar tres tipos genéricos de servidores: servidores físicos, servidores virtuales (una o varias particiones en un servidor para dedicarlo a prestar varios servicios) y servidores en la nube
10	Centro de redes y cableado	comprende toda la infraestructura de red con que cuenta una organización y que se encuentra distribuida en sus diferentes dependencias. Dentro de esta categoría encontramos centros de cableado, equipos de red activos y pasivos y todo el tendido de red que interconectan los diferentes dispositivos que tiene la organización.
11	Centro de computo	también llamado centro de procesamiento de datos, centro de datos o data center, es aquel sitio o sitios donde tradicionalmente las organizaciones concentran los dispositivos de computo más críticos a través de los cuales se centraliza el procesamiento y almacenamiento de la información considerada más crítica para el negocio
12	Energía	Son todos aquellos servicios y dispositivos que permiten que un dispositivo físico de procesamiento de información pueda operar, si se tiene en cuenta que casi en su totalidad hoy dependen de la energía eléctrica. Dentro de esta categoría también se encuentran los dispositivos que permiten generar energía alterna, y que permiten su adecuado resguardo, tal es el caso de los bancos de baterías y las UPS. Esta capa tecnológica es una de las capas más importantes, por no decir la más importante de la infraestructura tecnológica de una organización, debido a que es la que permite que las demás capas puedan cumplir su función
13	Recurso Humano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

Figura 8. Capas de Tecnologías de Información y Comunicaciones

Fuente: F. J. Valencia Duque, *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000*. 2021.

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Figura 9. Criterios de Índice de Información Clasificada y Reservada

Fuente: MinTIC, "Guía para la Gestión y Clasificación de Activos de Información." 2016

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Figura 10. Clasificación de la Confidencialidad

Fuente: MinTIC, "Guía para la Gestión y Clasificación de Activos de Información." 2016

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Figura 12. Clasificación de la integridad

Fuente: MinTIC, "Guía para la Gestión y Clasificación de Activos de Información." 2016

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Figura 11. Clasificación de la Disponibilidad

Fuente: MinTIC, "Guía para la Gestión y Clasificación de Activos de Información." 2016

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Figura 13. Niveles de Clasificación de la Criticidad

Fuente: MinTIC, "Guía para la Gestión y Clasificación de Activos de Información." 2016

6.2.3.2. Objetivos y planes para lograrlo

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.

A continuación, se presenta el plan para fortalecer la implementación del modelo de seguridad y privacidad del INVAMA:

Tabla 5. Plan implementación del modelo de seguridad y privacidad de información del INVAMA

Actividad	Descripción	Fecha Inicial	Fecha Final	Responsable
Recolección y revisión de bases de datos personales	Registrar o actualizar las bases de datos personales.	01-02-2024	28-02-2024	Responsable de Seguridad y Privacidad de la Información

Calle 3C#22-92 · Barrio Alcázares · Manizales
Tel: (6)8891030 · www.invama.gov.co

				Líderes de Procesos
Actualizar las políticas de seguridad y privacidad de la información	Definir y establecer un conjunto de políticas para la seguridad y privacidad de la información, aprobada por la dirección, publicada y comunicada a las partes interesadas de la entidad.	01-03-2024	31-03-2024	Responsable de Seguridad y Privacidad de la Información Comité directivo (alta dirección)
Actualizar los activos de seguridad de la información.	Actualizar en el modelo de seguridad de la información los activos de seguridad de la información, teniendo en cuenta la criticidad desde disponibilidad, integridad y confidencialidad	01-04-2024	30-04-2024	Responsable de Seguridad y Privacidad de la Información
Realizar la identificación, análisis y valoración de Riesgos de Seguridad de la Información y el tratamiento de riesgos de los mismos.	Actualizar el análisis y valoración de riesgos de la seguridad de la información y el tratamiento de riesgos de los mismos.	01-05-2024	30-05-2024	Responsable de Seguridad y Privacidad de la Información
Aceptación de los riesgos de Seguridad de la Información.	La revisión del plan de tratamiento de los riesgos y la evaluación del riesgo residual, debe ser aceptada por la alta dirección de manera formal	01-06-2024	30-06-2024	Comité directivo (alta dirección)
Ajuste y/o creación de procedimientos de la entidad en lo relacionado a seguridad de la información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	01-08-2024	31-08-2024	Responsable de Seguridad y Privacidad de la Información

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

				Líderes de Proceso
Establecer el proceso de gestión de incidentes de seguridad de la información	Establecer el proceso de gestión de incidentes de seguridad para proveer en la entidad un mecanismo para el reporte, evaluación y respuesta a los eventos e incidencias de seguridad de la información; como también la implementación o ajustes necesarios a procedimientos necesarios identificados en la declaración de aplicabilidad.(Basado en la norma ISO 27035)	01-07-2024	31-07-2024	Responsable de Seguridad y Privacidad de la Información
Continuidad del negocio y recuperación de desastres	Actualización del plan de continuidad de negocio y recuperación de desastres	01-09-2024	31-08-2024	Responsable de Seguridad y Privacidad de la Información Responsable de TI
Indicadores de medición del SGSI	Formular, implementar y actualizar los indicadores del SGSI	01-10-2024	31-10-2024	Responsable de Seguridad y Privacidad de la Información
Afinamiento del DataCenter	El servicio proporcionado le permitirá a la Entidad realizar una revisión y optimización de sus servicios del centro de datos, el cual se encuentra cubierto y	01-03-2024	31-12-2024	Responsable de TI Responsable de Seguridad y Privacidad de la Información

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

	soportado por el área interna de TI.			
Migración IPV4 a IPV6	Realizar la migración de IPv4 a IPv6 de los componentes tecnológicos del INVAMA	01-06-2024	31-12-2024	Responsable de TI Responsable de Seguridad y Privacidad de la Información
Capacitación, sensibilización y comunicación de Seguridad de la Información.	Asegurar que los funcionarios y contratistas de la Entidad cuenten con los conocimientos, educación y formación de seguridad y privacidad de la información.	01-03-2024	31-12-2024	Responsable de Seguridad y Privacidad de la Información Área Comunicación y Prensa Área de Gestión Humana

Fuente: Propia

6.2.4. Soporte

6.2.4.1. Recursos

La Entidad debe determinar y proporcionar los recursos para adoptar el SGSI, teniendo en cuenta que es un proceso trasversal de la Entidad, se requiere que se disponga de los recursos financieros, humanos y de cualquier otro recurso que permita la adopción implementación mantenimiento y mejora continua del SGSI.

Por tal motivo se debe incluir dentro de los proyectos de inversión de la Entidad aquellas actividades relacionadas con la adopción del Sistema de Seguridad y Privacidad de la Información.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6.2.4.2. Competencia, Sensibilización y Comunicación

De acuerdo a la guía 14 “Capacitación, Sensibilización y Comunicación de Seguridad de la Información del MinTIC”, se define un plan de comunicación, capacitación, sensibilización y concientización para la Entidad, con el fin de:

- Determinar las necesidades de comunicación interna relacionadas con la seguridad y privacidad de la información
- Asegurar que los funcionarios y contratistas de la Entidad cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
- Concientizar a los funcionarios, contratistas y terceros en la importancia de la protección de la información.

Las temáticas a abordar son:

- Conocimiento general del sistema de gestión de seguridad de la información.
- Conocimiento de la Política de seguridad de la Información
- Amenazas informáticas
- Generalidades sobre regulación en materia de seguridad de la información
- Atención y respuesta a incidentes de seguridad de la información
- Uso de contraseñas.
- Protección contra los virus.
- Instrucciones al uso del correo electrónico e identificación de Correos Sospechosos
- Uso Apropiado de Internet.
- Política De Escritorio Limpio
- Backup de la información.
- Seguridad de los equipos.

6.2.4.3. Documentación

La Entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación y de acuerdo al

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

procedimiento que tiene la Entidad GD-GC-PR-01 Generación y control de documentos y registros de calidad.

6.3. FASE DE IMPLEMENTACIÓN

Esta Fase IMPLEMENTACION en la norma ISO 27001:2022, capítulo 8 - Operación, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

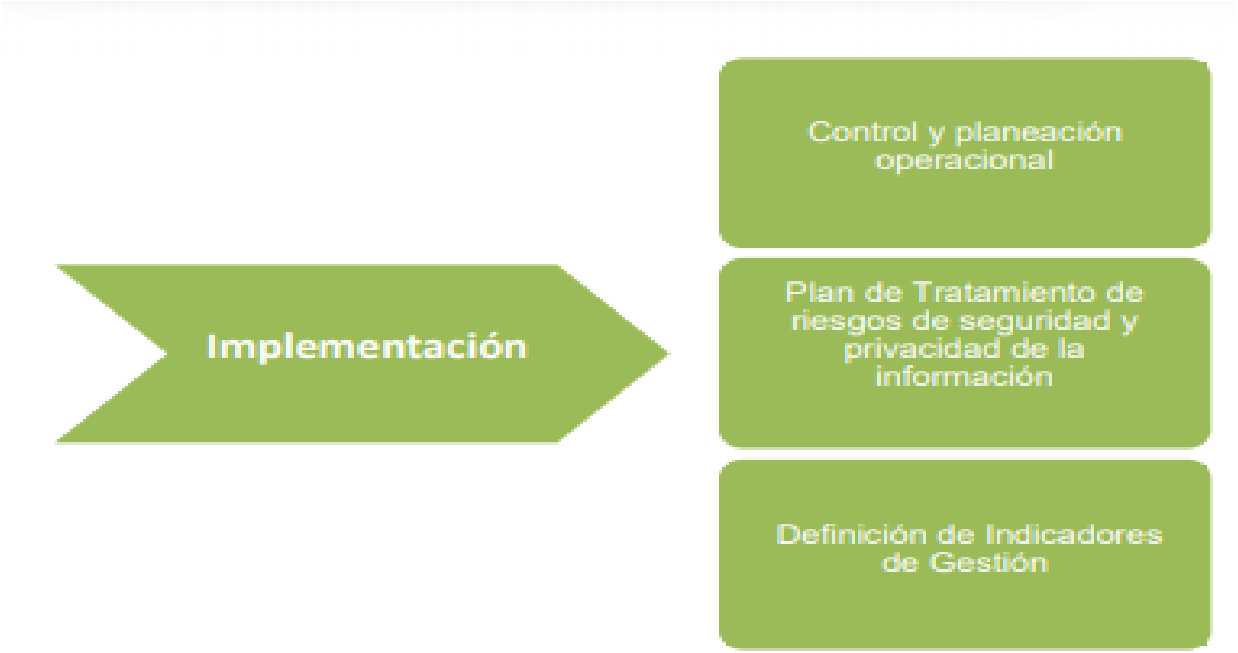

Figura 14. Fase de Implementación

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

6.3.1. Control y planeación operacional

La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos definido en la "Matriz de Riesgos", esta información debe estar documentada según lo planificado. Estos documentos deben ser aprobados por el Comité Institucional de Gestión y Desempeño (MIPG).

6.3.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El plan de tratamiento de riesgos del Instituto de Valorización de Manizales – INVAMA https://invama.gov.co/wp-content/uploads/2023/02/Plan-Tratamiento-de-Riesgos-Seguridad-de-la-Informacion-2023.pdf se encuentra aprobado y publicado.

6.3.3. Definición de Indicadores de Gestión

Se presenta una propuesta de indicadores “Indicadores del SGSI.xlsx”, basados en la guía 9 del MinTIC, los cuales deben ser conocidos y aceptados por el Comité de Gestión Institucional y Desempeño como lo establece el MIPG.

6.4. FASE DE EVALUACIÓN

La Fase EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2022 descrita en el capítulo 9 - Evaluación del desempeño, define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

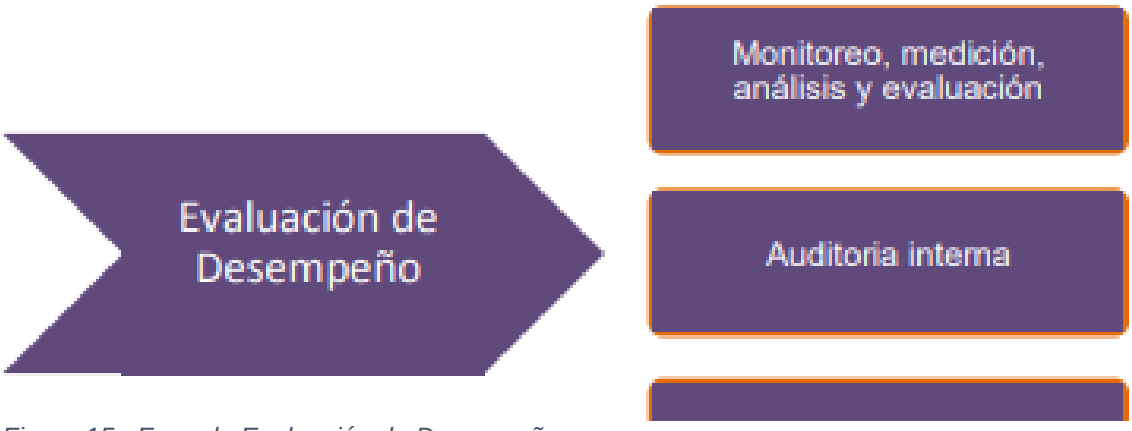

Figura 15. Fase de Evaluación de Desempeño

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

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6.4.1. Monitoreo, Medición, Análisis y Evaluación

La Entidad debe evaluar la gestión, cumplimiento y el desempeño de la seguridad de la información y la eficacia del sistema de gestión de seguridad de la información en un término de seis (6) meses.

6.4.2. Auditoria Interna

La Entidad debe solicitar al área de Control Interno, incluir en el programa anual de auditorías, la auditoría de seguridad y privacidad de la información como mínimo una (1) vez al año, con el fin de obtener información sobre el cumplimiento del SGSI. Así mismo, informar a las partes interesadas, los resultados de la ejecución de las auditorías.

6.4.3. Revisión por la Alta Dirección

La Organización debe ampliar el alcance del proceso PG-RD-PR-01 Revisión por la Dirección, el cual incluya por lo menos una (1) vez al año la revisión del SGSI de la Entidad, por parte de la Alta Dirección, que determine la conveniencia, adecuación y eficacia del SGSI, de tal forma que la Entidad tome las acciones necesarias para mejorar el sistema, y en consecuencia la seguridad de los activos de información.

Las actividades que se deben llevar a cabo en la revisión por la dirección son:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del SGSI.
- Seguimiento al alcance y a la implementación del SGSI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del SGSI

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del SGSI)

6.5. FASE DE MEJORA CONTINUA

Esta Fase mejora continua en la norma ISO 27001:2022. En el capítulo 10 Mejora, se establece para el proceso de mejorar el sistema de gestión de seguridad y privacidad de la información, la inconformidad que ocurra en la entidad debe establecer las acciones más efectivas para solucionar y evaluar la necesidad de acción para eliminar el error y lograr el objetivo de que no se repita.

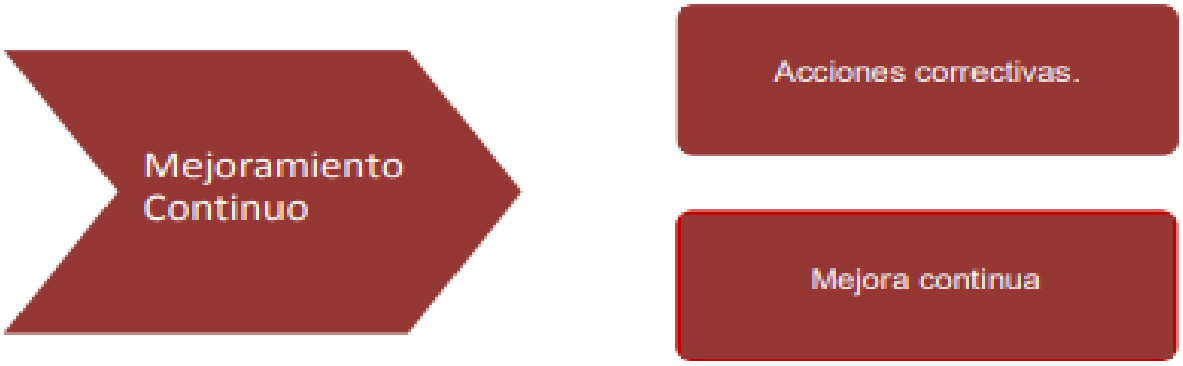

Figura 16. Fase de Mejoramiento Continúo

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

6.5.1. Acciones correctivas

La Entidad debe efectuar el plan de mejoramiento de las no conformidades de las auditorías internas realizadas con el fin de eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

6.5.2. Mejora continua

Es importante que la Entidad defina y ejecute el plan de mejora continua con base en los resultados de evaluación del desempeño (indicadores, auditorías internas, revisión por la Dirección). Este plan debe incluir:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el SGSI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al SGSI.

Estos insumos tendrán como resultado un plan de mejoramiento continuo, revisados y aprobados por la Alta Dirección de la Entidad.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

7. DOCUMENTOS DE REFERENCIA

Ministerio de Tecnologías de Información, Modelo de Seguridad de la Información, disponible en https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Ministerio de Tecnologías de Información, Modelo de Gestión de Riesgos de Seguridad digital.

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co

CONTROL DE CAMBIOS

VERSIÓN	FECHA DEL CAMBIO	DESCRIPCIÓN DE LA MODIFICACIÓN
0	20-01-2020	Creación del documento
1	27-01-2021	Ajuste documento actividades y fechas
2	27-01-2022	Ajustes al documento
3	31-01-2023	Se actualiza marco normativo y se actualiza actividades
4	23-01-2024	Se actualiza objetivos específicos, justificación, normatividad, fases del Modelo de Seguridad y Privacidad de la Información, actividades y fechas.

FIRMAS Y REVISIONES

	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	DIANA LORENA CORTÉS JIMÉNEZ	Técnico Administrativo Sistemas	23-01-2024	
APROBÓ	JAIRO ALFREDO LÓPEZ BAENA	Gerente	25-01-2024	

Calle 3C#22-92·Barrio Alcázares·Manizales
Tel:(6)8891030·www.invama.gov.co