Plan de Seguridad y Privacidad de la Información

2022

Instituto de Valorización de Manizales

INVAMA

Manizales, Enero de 2022

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

FIRMAS Y REVISIONES

	NOMBRE	CARGO	FECHA	FIRMA
ELABORÓ	Diana Lorena Cortés Jiménez	Técnico Administrativo Sistemas	27-01-2022	
APROBÓ	Mauricio Cárdenas Ramírez	Gerente	28-01-2022	

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

TABLA DE CONTENIDO

INTRODUCCION 1
1. OBJETIVO 3
2. ALCANCE 4
3. MARCO NORMATIVO 5
4. GLOSARIO 9
5. ROLES Y RESPONSABILIDADES 15
6. PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 21
DOCUMENTOS DE REFERENCIA 26

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

1. OBJETIVO

Describir las actividades del Plan de Seguridad y Privacidad de la Información, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI – del Instituto de Valorización de Manizales – INVAMA.

1.1. OBJETIVOS ESPECÍFICOS

- 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 y personal en comisión de la Presidencia de la República).
- Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.
- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

2. 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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

3. 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.
- **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.
- **Decreto 1747 de 2000**. Reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
- **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 1273 de 2009. Código Penal.** Se crea un nuevo bien jurídico titulado “De la Protección de la Información y de los Datos”.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

- **Decreto 235 de 2010.** Se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

- **Decreto 2952 de 2010.** Reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
- **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.
- **Decreto 2364 de 2012. Firma Electrónica.** Establece la reglamentación del artículo 7 de la ley 527 de 1999.
- **Decreto 2609 de 2012**. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos en las entidades del Estado.
- **Ley 1581 de 2012. Protección de Datos Personales.** Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
- **Decreto 1377 de 2013. Reglamentar parcialmente la Ley 1581 de 2012**. Reglamenta aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

- **Decreto 0032 de 2013. Creación de la Comisión Nacional Digital y de Información Estatal.** El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el documento CONPES 3701, creó, a través de este decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.
- **Decreto 886 de 2014. Registro Nacional de Bases de Datos.** Reglamenta la información mínima que debe contener este registro, así como los términos y condiciones bajo las cuales se deben inscribir los responsables del tratamiento.
- **Ley 1712 de 2014**. Ley de transparencia y del derecho de acceso a la información pública.
- **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 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.
- **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

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

- **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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

4. 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)

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

- **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

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

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

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

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

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

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

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

- **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).

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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).

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

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

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

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

- **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original. (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).

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

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

- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa,

  Políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

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

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

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

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

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

5. ROLES Y RESPONSABILIDADES

Rol	Descripción del Rol	Funciones
Comité directivo (alta dirección)	Responsable de revisar el Sistema de Gestión 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). ✓ Asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.
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, así como de Aprobar el plan de mitigación de riesgos del SGSI.	✓ Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad. ✓ Revisar los diagnósticos del estado de la seguridad de la información en la Entidad. ✓ Acompañar e impulsar el desarrollo de proyectos de seguridad. ✓ Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Entidad. ✓ Recomendar roles y responsabilidades específicos que

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

		se relacionen con la seguridad de la información. ✓ Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. ✓ Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. ✓ Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. ✓ Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. ✓ 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.
Responsable de Seguridad y Privacidad de la Información **	Responsable de coordinar todas las actividades relacionadas con la gestión de la seguridad de la información.	✓ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad. ✓ Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. ✓ Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. ✓ Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

		de seguridad de gestión de TI e información. ✓ Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. ✓ Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. ✓ Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. ✓ Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. ✓ Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. ✓ Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. ✓ Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

		✓ Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. ✓ Consolidar la información de Base de datos personales que maneja o tiene la entidad.
Responsable de TI	Responsable de planificar, organizar, coordinar, gestionar, controlar la estrategia de uso y apropiación de TI.	✓ Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. ✓ Participar en la elaboración del cronograma de capacitación de seguridad digital en la Entidad. ✓ Identificar y reportar riesgos, eventos o incidentes de ciberseguridad a través de los canales definidos. ✓ Coordinar la administración, configuración de los recursos informáticos dentro de la plataforma tecnológica de seguridad. ✓ Planear y ejecutar el plan de mantenimiento y actualización de la infraestructura tecnológica y de telecomunicaciones de la entidad.
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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

Usuarios de la Información (Funcionarios, Contratistas, Terceros)	Personas que utilizan la información y los activos tecnológicos en la Entidad para la normal ejecución de sus procesos.	✓ Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. ✓ Cumplir a cabalidad con las políticas, lineamientos y procedimientos de seguridad y privacidad de la información definida y aprobada. ✓ Comunicar al responsable de Seguridad de la Información de las anomalías o incidentes de seguridad, así como de las situaciones sospechosas. ✓ Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos. ✓ Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información.
Auditores SGSI	Responsable de revisar el cumplimiento del SGSI	✓ Llevar a cabo auditorías internas a intervalos planificados con miras a proporcionar información acerca del estado actual del Sistema de Gestión de Seguridad de la Información.
Área Jurídica y Contratación		✓ Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. ✓ Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

Área de Gestión Humana		✓ 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.

*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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

6. PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El Instituto de Valorización de Manizales – INVAMA -, buscando desarrollar el Modelo de Seguridad y Privacidad de la Información (MSPI) ha establecido una estrategia integral de aseguramiento de la información de forma tal que su adopción se está realizando de forma integrada con el Sistema de Gestión de Seguridad de la Información, considerando que la norma ISO/IEC 27001:2013 es base de ambos sistemas y que las guías técnicas desarrolladas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, se basan en dicha norma y consideran el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Actividad	Descripción	Fecha Inicial	Fecha Final	Responsable
Definición de roles y responsabilidades	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad	01-02-2022	31-03-2022	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,	01-04-2022	31-12-2022	Responsable de Seguridad y Privacidad de la Información

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

	integridad y confidencialidad			
Actualizar el 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.	01-04-2022	31-12-2022	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	01-04-2022	31-12-2022	Comité directivo (alta dirección)
Establecimiento de 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.	01-04-2022	31-12-2022	Responsable de Seguridad y Privacidad de la Información 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.	01-02-2022	31-12-2022	Responsable de Seguridad y Privacidad de la Información Líderes de Proceso

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

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.	01-04-2022	31-12-2022	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 soportado por el área interna de TI.	01-04-2022	31-12-2022	Responsable de TI Responsable de Seguridad y Privacidad de la Información
Migración IPV4 a IPV6	Realizar la migración de IPv4 a IPv6 de los componentes tecnológicos del INVAMA	01-02-2022	31-12-2022	Responsable de TI 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	01-02-2022	31-12-2022	Responsable de Seguridad y

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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

				Privacidad de la Información Responsable de TI
Monitoreo y Revisión del Riesgo en la Seguridad de la Información	Monitorear y revisar los factores de riesgos, con el fin de detectar cambios en el contexto interno y externo de la Entidad.	01-04-2022	31-12-2022	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.	01-04-2022	31-12-2022	Responsable de Seguridad y Privacidad de la Información Área Comunicación y Prensa Área de Gestión Humana
Incluir en el comité de Gestión y Desempeño los temas de seguridad y privacidad de la información	Incluir en el comité de Gestión y Desempeño los temas de seguridad y privacidad de la información	01-03-2022	31-12-2022	Comité directivo (alta dirección) Comité Institucional

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

				de Gestión y Desempeño
plan de aplicación y mejora continua del Sistema de Gestión de Seguridad y privacidad de la Información - SGSI	Se ejecutará el cronograma de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información - SGSI el cual consiste en el desarrollo de las tareas correspondientes a la vigencia 2022, como la verificación por parte de la alta dirección del SGSI, cumplimiento de los objetivos e indicadores definidos para el sistema y apoyo al Plan de Transformación Digital.	01-04-2022	31-12-2022	Responsable de Seguridad y Privacidad de la Información

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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.

ILUMINAMOS Y PROYECTAMOS TU FUTURO.

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