ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

IPES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE DISEÑO Y ANÁLISIS ESTRATÉGICO

Bogotá, 2024

Elaboró:	Revisión:	Aprobó:
Daniel Ernesto Fragoso Amariz Profesional Universitario SDAE Martha Patricia Mateus Profesional Contratista SDAE	Sandy Patricia Guerrero Salcedo Contratista 064 de 2023	Paola Rico Parada Subdirector de Diseño y Análisis Estratégico - SDAE

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

1. INTRODUCCIÓN

La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en un entorno cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad de redes y sistemas de información).

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de estos activos contra una gran variedad de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplen los objetivos específicos de seguridad de la organización. Esto debería hacerse en conjunto con otros procesos de gestión. Argumento por el cual se realiza el documento, describir las razones, naturaleza e interés del documento y si es necesario referenciar el marco normativo.[1]

2. JUSTIFICACIÓN

La seguridad de la información es importante tanto para los negocios del sector público como del privado y para proteger la infraestructura crítica. En ambos sectores, la seguridad de la información actuará como un elemento facilitador para lograr, por ejemplo, gobierno en línea (e-government) o negocios electrónicos (e-business) y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y compartir los recursos de información incrementan la dificultad para lograr el control del acceso. La tendencia hacia la computación distribuida también ha debilitado la eficacia del control central y especializado.[2]

La definición, implementación y seguimiento del plan de seguridad de la información en el Instituto para la Economía Social - IPES, permitirá la toma de decisiones oportunas, encaminadas a desarrollar seguridad y privacidad de la información de manera apropiada, derivada de la evaluación de riesgos, el cumplimiento normativo y los requisitos de la entidad para el procesamiento de la información que apoya el cumplimiento de su misión.

[1] Instituto colombiano de Normas Técnicas- ICONTEC Norma Técnica Colombiana NTC-ISO/IEC27002- 2013- 0. Introducción, 0.1. ¿Qué es la Seguridad de la Información?, edición digital, pág. 11.

[2] Instituto colombiano de Normas Técnicas- ICONTEC Norma Técnica Colombiana NTC-ISO/IEC27002- 2013- 0. Introducción, 0.2. ¿Por qué es Necesaria la Seguridad de la Información?, edición digital, pág. 11.

3. OBJETIVOS

Este documento tiene como propósito definir el plan de seguridad y privacidad de la información en el Instituto para la Economía Social, que permita realizar el seguimiento en la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información - SGSI, considerando los lineamientos y directrices establecidas en el Modelo de Seguridad y Privacidad de la Información – MSPI y el Modelo de Planeación y Gestión – MIPG. Establece las responsabilidades en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la entidad. Asimismo, orienta a los funcionarios, contratistas y terceros sobre la responsabilidad en el uso y buen manejo de los activos de información y de la infraestructura tecnológica que soporta la operación de la entidad.

El Plan de Seguridad y Privacidad de la Información propende por la preservación de la confidencialidad, integridad, disponibilidad de la información en la entidad, permitiendo garantizar la privacidad de los datos, y brindando confianza en su gestión.

El plan tiene como objetivo diseñar, generar e implementar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la entidad alineado al Modelo de Seguridad y Privacidad de la información, al plan de seguridad y privacidad de la información con la finalidad de fortalecer el aseguramiento de los servicios TI y preservar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad y los usuarios.

Los objetivos específicos son:

a. Comunicar e implementar la estrategia de seguridad de la información.
b. Incrementar el nivel de madurez en la gestión de la seguridad de la información en la entidad
c. Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
d. Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
e. Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
f. Fomentar la conciencia alrededor de la importancia en el aseguramiento de la información institucional, la cual debe ser adoptada como una cultura organizacional.

4. ALCANCE

El plan de seguridad y privacidad de la información aplica para la definición, implementación, mantenimiento y mejora de los lineamientos, directrices, políticas y controles de seguridad de la información que permiten al Instituto para la Economía Social – IPES contar con niveles apropiados de seguridad de los activos de información.

Este plan se encuentra en el marco de las directrices dadas en la dimensión Gestión con Valores para Resultado de MIPG y las políticas de Gobierno Digital y Seguridad Digital.

5. RESPONSABILIDADES

El proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos es responsable de realizar seguimiento, actualización, mantenimiento y mejora del plan de seguridad y privacidad de la información del Instituto para la Economía Social – IPES.

5.1. COMITÉ DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

El Articulo 47 de la Resolución 492 de 2021 establece que: “El propósito del Comité de Sistemas y Seguridad de la Información es establecer lineamientos, directrices, controles y en general la consolidar el uso apropiado de los servicios de procesamiento de información, que permitan la protección de los activos de información institucional en el marco normativo vigente.

El Articulo 49 de la Resolución 492 de 2021 establece que: Funciones del Comité de Sistemas y Seguridad de la Información. Los integrantes del Comité deberán cumplir con las siguientes funciones:

1. Aprobar el plan estratégico de tecnologías de la información y las comunicaciones
2. Definir políticas de desarrollo y seguridad de la información
3. Establecer acciones que mitiguen riesgos de perdida que comprometan los recursos de información.
4. Fijar acciones específicas que ayuden a proveer un ambiente seguro y estable de recursos de información, que sea consistente con las metas, políticas y objetivos del Instituto para la Economía Social – IPES
5. Garantizar que se provea de los recursos humanos, técnicos y financieros para asegurar que la información del Instituto se encuentre protegida apropiadamente, sobre los presupuestos de la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos y físicos que la soportan.
6. Impulsar la Implementación del Sistema de Gestión de Seguridad de la Información -SGSI-
7. Revisar el diagnóstico del estado de la seguridad de la información en la Entidad
8. Evaluar los requerimientos tecnológicos en materia de Tecnología de Información y Comunicaciones
9. Definir roles y responsabilidades que se relacionen con la seguridad de la información
10. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información
11. Establecer las estrategias para la divulgación y comunicación de las políticas y normas que el IPES, dicte en materia de seguridad de la información.

12. Definir la responsabilidad en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la Entidad.
13. Definir aspectos a ser tenidos en cuenta por la entidad, relacionados con el talento humano y su responsabilidad en el uso de la información institucional antes, durante y en la terminación de la vinculación laboral.
14. Establecer directrices para la protección física de los activos de infraestructura tecnológica de la entidad
15. Establecer responsabilidades, controles y lineamientos en procura de proteger los sistemas y servicios informáticos por medio de los cuales se procesa la información institucional, que garanticen la operación informática de la entidad.
16. Fomentar la conciencia alrededor de la importancia en el aseguramiento de la información institucional, la cual debe ser adoptada como una cultura organizacional.
17. Las demás funciones inherentes a la naturaleza del Comité
18. Gestionar el acta y los soportes dirigido al Comité Institucional de Gestión y Desempeño de la gestión y seguimiento del Comité de Sistemas y Seguridad de la Información por cada sesión realizada, citando las conclusiones, indicadores y recomendaciones de la sesión generadas, adjuntando, la lista de asistencia, presentación y con copia a la secretaria técnica del Comité Institucional de gestión y Desempeño.

5.2 ROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL IPES

5.2.1 Oficial de Seguridad de la Información

El Comité de Sistemas y Seguridad de la Información, designará al oficial de seguridad de la información, el cual tiene como obligaciones principales:

- Diseñar y presentar para aprobación políticas, directrices y lineamientos encaminados a fortalecer la seguridad de la información.
- Identificar el grado de madurez en la implementación del Modelo de Seguridad y Privacidad de la Información en la entidad.
- Coordinar las actividades correspondientes a la gestión de incidentes de seguridad, con la finalidad de contar con un enfoque estructurado y planificado que permita su manejo adecuado, así como la presentación al Comité de Sistemas y Seguridad de la Información de los incidentes de seguridad de la información presentados y las acciones tomadas para reducir su impacto.
- Establecer estrategias de defensa proactivas y reactivas.
- Liderar la implementación y mantenimiento del SGSI velando por el cumplimiento de sus lineamientos.
- Desarrollar, mantener actualizadas y comunicar las políticas, estándares y guías de seguridad de la información, especialmente, aquellas con un enfoque tecnológico.
- Coordinador el proceso de gestión de riesgos de seguridad digital y coordinar el plan para la mitigación de los mismos.
- Elaborar o coordinar actividades de entrenamiento y sensibilización en seguridad de la información y el SGSI.
- Administrar, monitorear y coordinar la seguridad de la información en la Entidad.

- Definir métodos que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la Entidad.
- Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a seguridad de la información.
- Documentar la actualización, el seguimiento, medición, análisis y evaluación del desempeño de la seguridad de la información y eficacia del SGSI.

El rol de **Oficial de Seguridad de la Información** será asumido por el subdirector (a) de Diseño y Análisis Estratégico, hasta tanto el comité haga oficial la designación del responsable a través de los medios dispuestos por la Entidad.

5.2.2 Responsable del tratamiento de los datos personales

En cumplimiento de los lineamientos establecidos en la Ley 1581 de 2012 *"Por la cual se dictan disposiciones generales para la protección de datos personales*", y la PL-021 Política de Tratamiento de Datos Personales, se define como responsable[3] del tratamiento[4] de datos personales el Instituto para la Economía Social, NIT: 899.999.446-0.

Los demás lineamientos establecidos por la Entidad para el tratamiento de datos personales se encuentran establecidos en la PL-021 Política de Tratamiento de Datos Personales versión 1 de fecha 24 enero de 2019.

5.2.3 Equipo de Gestión

El equipo de gestión del proyecto se encarga de tomar las medidas para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad y Privacidad de la Información, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

En el marco del desarrollo de las actividades asociadas al SGSI, teniendo en cuenta la estructura de la Subdirección de Diseño y Análisis Estratégico -SDAE-, el proceso de Gestión de la Información y Recursos Tecnológicos, es responsable de definir, implementar, mantener y mejorar el SGSI.

El proceso se encuentra operando funcionalmente con la siguiente estructura *-no oficial-:*

[3] *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*

[4] *Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*

Ilustración 2. Roles Proceso de Gestión de la Información y RecursosTecnológicos

5.3 ROLES Y RESPONSABILIDADES EQUIPO DE GESTIÓN

Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la Entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal, y que no dependa exclusivamente de la oficina o área de TI.[5]

5.3.1 Administrador Infraestructura Tecnológica

Garantizar la continuidad en la prestación de los sistemas y servicios informáticos que apoyan el cumplimiento de los objetivos y la misión de la Entidad, a través de la administración (configuración, pruebas, puesta en operación, migración, actualización, mantenimiento) de la infraestructura tecnológica IT que soportan la operación informática institucional.

El responsable de la administración de los activos de IT, debe mantener actualizada la documentación requerida para garantizar la disponibilidad de los servicios informáticos críticos (HEMI, GOOBI, recursos compartidos, file server), que incluye manuales de usuario, manuales de configuración, despliegue, consolas y medios de instalación, códigos fuente (cuando aplique) y la información para la puesta en operación (IP, servidores, motores de DB y sistemas operativos).

En desarrollo de la administración de los activos de IT que soportan la operación informática de la entidad, se deben establecer estrategias que permitan contar con respaldo del recurso humano (backup), quién podrá, de ser necesario, solucionar inconvenientes técnicos asociados a los dispositivos de tecnologías de información y comunicaciones.

El administrador de la IT debe gestionar (documentar) los incidentes de seguridad de la información materializados, que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información, así como alimentar la base de conocimiento de las acciones adelantadas para restaurar la operación.

[5] articles-5482_G4_Roles_responsabilidades 6.2 Equipo de gestión

Responsable: Profesional Subdirección de Diseño y Análisis Estratégico -SDAE
Apoyo: Proveedores y terceros

5.3.2 Seguridad Informática

Buscar el aseguramiento de la información institucional digital, creada, procesada, modificada y alojada en la infraestructura tecnológica de la entidad, a través de la definición e implementación del SGSI, MSPI, seguimiento, monitoreo, mantenimiento y mejora continua de los controles, lineamientos y directrices de seguridad informática en concordancia con las normas técnicas internacionales como por ejemplo NTC-ISO-IEC 27001:2013 y normatividad vigente y aplicable.

El encargado de la seguridad informática del equipo de sistemas, es responsable de realizar seguimiento a la documentación asociada al MSPI y SGSI, la cual debe estar debidamente versionada, actualizada, aprobada y controlada en el marco del Sistema Integrado de Gestión y el Modelo Integrado de Planeación y Gestión – MIPG.
La ejecución de campañas de socialización que busquen generar una cultura alrededor de la seguridad de la información en el Instituto, es responsabilidad encargado del presente rol, incluyendo la definición y seguimiento definidos en conjunto con los integrantes del equipo del proyecto.

Responsable: Profesional Subdirección de Diseño y Análisis Estratégico -SDAE
Apoyo: Proveedores y terceros

5.3.3 Administrador Redes de Comunicaciones

Los servicios informáticos, red de datos y de comunicaciones deben contar con altos niveles de disponibilidad, que se reflejen en oportunidad de la información institucional de manera eficiente y efectiva, para lo cual se debe gestionar el recurso humano calificado para adelantar actividades de administración, configuración, mantenimiento y operación de los equipos de comunicaciones de la entidad. Es responsabilidad del administrador de las redes de datos (networking) y los equipos que la soportan, implementar, mantener y mejorar las mejores prácticas y estándares para la gestión de infraestructura tecnológica.

El administrador de redes, debe ejecutar las acciones necesarias asociadas a la continuidad en la prestación los servicios informáticos en la Entidad, adelantando tareas de respaldo de la configuración de los equipos activos, así como gestionar garantías sobre los activos de infraestructura tecnológica clasificados y valorados como críticos.

- Se deben proponer alternativas de operación en caso de materialización de incidentes de seguridad que comprometan total o parcialmente la operación informática.

Responsable: Profesional Subdirección de Diseño y Análisis Estratégico -SDAE
Apoyo: Proveedores y terceros

5.3.4 DBA- Administrador de Bases de Datos

Garantizar la protección de los datos creados, procesados y/o modificados que se encuentran alojados en los sistemas de información de la entidad, a partir de la implementación, mantenimiento y mejora de controles de seguridad que permitan niveles apropiados de integridad y confiabilidad de la información resultado de la operación informática misional de la entidad.

La responsabilidad en la administración de las bases de datos misionales de la Entidad, es asumida desde la SDAE a través del proceso de Gestión de la Información y Recursos Tecnológicos, considerando como críticos las tareas de procesamiento y manejo de la información institucional usada en la toma de decisiones encaminadas al cumplimiento de metas, objetivos y la misión del IPES.

El administrador de las bases de datos debe garantizar que exista una única fuente de información institucional, para lo cual se establecerá un único sistema de reportes misional, operado a través del documento institucional vigente “Procesamiento de Datos”. La asignación de un único DBA en el IPES, permite a la Entidad contar con niveles de confiabilidad de la información reportada ante entes de control, reportes de metas y demás instancias que lo requieran.

Responsable: Profesional Subdirección de Diseño y Análisis Estratégico -SDAE
Apoyo: Proveedores y terceros

5.3.5 Administración Sistema de Información Misional – HEMI

Uno de los logros de la Política de Gobierno Digital, se relaciona con los sistemas de información y busca potenciar los procesos y servicios que presta la Entidad a través de la gestión de los sistemas de información.

Es responsabilidad del administrador de la herramienta misional HEMI, contar con la documentación (modelo ER, diccionario de datos, manuales de usuario, manuales de configuración…) debidamente actualizados y controlados, teniendo en cuenta los lineamientos de seguridad de la información para la publicación de documentos y requisitos del modelo integrado de planeación y gestión.

Las necesidades de ajustes, desarrollos nuevos e implementación de funcionalidades sobre la herramienta misional HEMI identificados y requeridos desde cada uno de los procesos (áreas, dependencias), deben ser evaluados y aprobados por el equipo de gestión de desarrollo, previa comunicación oficial por parte del área solicitante, a través del formato “Ajustes en los sistemas de información”, en cumplimiento de lo dispuesto en el procedimiento *“Gestión de cambios sobre los sistemas de información”.*

Los cambios que se hagan a las funcionalidades de la herramienta, deben ser aprobados por el líder del proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos, previa validación y documentación de las pruebas realizadas, así como planes de contingencia y recuperación.

El sistema de información misional es la fuente oficial de información institucional relacionada con la población objeto de atención, para lo cual las solicitudes de procesamiento de información, deben ser canalizadas a través de los medios oficiales

dispuestos para tal fin; es responsabilidad del administrador de este sistema dar estricto cumplimiento a los lineamientos dispuestos por el Comité de Sistemas y Seguridad de la Información, referentes al procesamiento de datos (generación de reportes).

Responsable: Profesional Subdirección de Diseño y Análisis Estratégico -SDAE
Apoyo: Proveedores y terceros

5.3.6 Administrador Sistemas de Información Administrativa

El equipo de sistemas de la SDAE, designará a los responsables de la administración, configuración y puesta en operación (cuando sea requerido) de los aplicativos que apoyan los procesos administrativos de la entidad, como nomina, inventarios, almacén, cartera y tesorería entre otros.

El administrador de los sistemas de información administrativo, es responsable de realizar seguimiento a la documentación requerida para su configuración, despliegue y puesta en operación, que permitan la oportuna recuperación frente a la materialización de un evento de seguridad informática que comprometa su operación.

Se deben aplicar procedimientos de copias de respaldo que permitan niveles apropiados de integridad de la información contenida en las bases de datos de los servicios informáticos administrativos, así como la ejecución de simulacros de restauración programados y controlados, que verifiquen la funcionalidad de las copias realizadas, para lo cual el administrador del sistema de información administrativa verificará los recursos (hw, sw, medios) necesarios y realizara la documentación de los resultados.

Importante: El equipo de sistemas de la SDAE es responsable de ejecutar acciones para preservar la disponibilidad de los sistemas de información administrativos, así como de velar por la protección de la información derivada de su uso. Los subdirectores, jefes de área, y jefes directos son responsables del uso de las herramientas, informando oportunamente al proceso de gestión de seguridad de la información y recursos tecnológicos a través del documento institucional vigente, roles y responsabilidades de los funcionarios designados. El uso de las funcionalidades de las herramientas informáticas de apoyo, es responsabilidad de los usuarios autorizados. Los usuarios son responsables por el manejo que den a las contraseñas asignadas, en cumplimiento de los lineamientos de seguridad de los activos de información del IPES, evitando exponerla a daño, modificación, destrucción accidental o intencional, robo o alteración.

Responsable: Subdirección Administrativa y Financiera - SAF **y** SDAE

5.3.7 Responsable Gestión documental

Desde el proceso de Gestión Documental, se debe velar por la clasificación de la información institucional. El responsable del proceso debe gestionar la implementación de un sistema de gestión documental que permita contar con seguimiento y trazabilidad en el flujo de activos de la información.

Responsable: Profesional Subdirección Administrativa y Financiera - SAF

5.3.8 Control de Documentos – SIG

El equipo del SIG, es responsable de garantizar el control de los documentos que consolidan el Sistema Integrado de Gestión del IPES. El responsable del SIG deberá verificar la estructura y forma de los documentos allegados por las diferentes dependencias de la Entidad, antes de avalar la publicación de los mismos.

Es responsabilidad del equipo del SIG, garantizar el control de los documentos generados al interior de la entidad, informando oportunamente a las áreas sobre la información vigente, a través de los medios electrónicos dispuestos.

Responsable: Profesional Subdirección de Diseño y Análisis Estratégico - SDAE

5.3.9 Responsable Plan de Sensibilización

Considerando la importancia de generar una cultura alrededor de la seguridad de la información en el Instituto para la Economía Social – IPES, desde el proceso de Gestión de la Información y Recursos Tecnológicos, la Oficina Asesora de Comunicaciones y demás áreas delegadas por el Comité de Sistemas y Seguridad de la Información, se debe establecer, actualizar y ejecutar un plan de comunicación que permita a la Entidad conocer los lineamientos y directrices relacionadas al SGSI.

Es responsabilidad de la Oficina Asesora de Comunicaciones apoyar el desarrollo de los planes de comunicación del SGSI y MSPI, en el marco de las actividades del Comité de Sistemas y Seguridad de la Información en cumplimiento de la resolución 492 de 2021.

6. CONDICIONES GENERALES

- Cumplimiento de los lineamientos para la administración de la seguridad y privacidad de la información de la Entidad.
- Utilizar la metodología propuesta por el Departamento Administrativo de la Función Pública y los lineamientos de ley establecidos para la seguridad y Privacidad de la Información.
- Cumplimiento a los lineamientos establecidos en el proceso de Gestión de la Información y Recursos Tecnológicos.

7. DEFINICIONES

1. **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital, dentro de los cuales se puede mencionar:
   - Información.

- Software.
- Recursos físicos.
- Servicios.
- Personas y sus cualificaciones, habilidades y experiencias.
- Elementos intangibles como la reputación y la imagen.

2. **Activo de información:** Conocimiento o datos que son de valor para la entidad. Ver modelo estándar de control interno para el Estado Colombiano, MECI 1000:2005, Numeral 2.2 Componente Información.

3. **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).

4. **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).

5. **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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

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

8. **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).

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

10. **Causas:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

11. **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

12. **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

13. **Control:** Medida que permite reducir o mitigar un riesgo. Entiéndase por 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.

14. **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).

15. **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) interacción entre usuarios.

16. **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).

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

18. **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

19. **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).

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

21. **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).

22. **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).

23. **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

24. **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)

25. **Evaluación del riesgo:** Busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

26. **Gestión del riesgo**: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

27. **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).

28. **Identificación del riesgo:** Se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

29. **Integridad:** Propiedad de exactitud y completitud

30. **Impacto**: Son las consecuencias que genera un riesgo una vez se materialice.

31. **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).

32. **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)

33. **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

34. **Política de administración de riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riego.

35. **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).

36. **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 GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

37. **Probabilidad:** Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo

38. **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

39. **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

40. **Riesgo de seguridad digital**: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos del ambiente físico, digital y las personas.

41. **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información. Además, puede involucrar otras propiedades como como: autenticidad, trazabilidad, no repudio y fiabilidad.

42. **Tolerancia al riesgo:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

43. **Tratamiento del riesgo:** Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

44. **Valoración de riesgos:** Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

45. **Vulnerabilidad:** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

8. DESARROLLO DEL PLAN

8.1. METODOLOGÍA

Para la definición del plan de tratamiento de riesgos de seguridad digital se señalan las actividades desarrolladas previamente:

- Comprensión del contexto.
- Identificación del riesgo.
- Análisis del riesgo inherente.
- Evaluación del riesgo.
- Definición de controles existentes.
- Análisis del riesgo residual.
- Selección de la opción de tratamiento del riesgo.
- Definición del plan de tratamiento.

El Instituto para la Economía Social – IPES se encuentra trabajando en la implementación del Sistema de Gestión de Seguridad de la Información – SGSI, y en su integración al Sistema Integrado de Gestión, por lo tanto, los riesgos identificados son los que pueden afectar la disponibilidad, integridad y confidencialidad de la información y las acciones definidas contribuyen a la preservación de estos principios de seguridad de la información. Las medidas que se implementarán serán comparadas con los controles del Anexo A de la NTC-ISO/IEC 27001:2013 a fin que no sean omitidos controles necesarios.

En el plan de tratamiento se determinan los siguientes ítems:

- **Opciones de manejo:** El propósito de esta etapa es seleccionar e implementar opciones o estrategias para abordar el riesgo y con base en ella diseñar las acciones a aplicar. Las opciones para el tratamiento de los riesgos son:

- **Reducir el riesgo** mediante la aplicación de controles apropiados de manera que el riesgo residual se pueda reevaluar como aceptable.
- **Asumir el riesgo** significa que se reconoce la exposición a la pérdida, pero no se toman acciones relativas a un riesgo en particular y la pérdida es aceptada, en caso de que ocurra.
- **Evitar el riesgo** la acción que da origen al riesgo particular.
- **Compartir o transferir el riesgo** a entidades como aseguradoras o proveedores que puedan gestionar de manera eficaz el riesgo particular, siempre que no resulte un costo superior al del riesgo mismo.

- **Acción para tratar el riesgo:** Describir las medidas o controles a implementar con el fin de lograr el tratamiento del riesgo.

- **Soporte:** Relaciona la evidencia que soportará el cumplimiento de la acción definida para tratar el riesgo.

- **Documentos asociados al control:** Describen los documentos existentes y que de alguna manera se relacionan con la implementación del control.

- **Responsable:** Proceso o rol encargado de la implementación y ejecución de las acciones que tratarán el riesgo.

- **Tiempo de ejecución:** Fechas de inicio y terminación de la implementación de las acciones.

- **Indicador**: Relaciona las métricas que miden la implementación de la acción.

9. DESARROLLO

9.1. COMPONENTES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se relacionan puntos críticos, en donde se pueden encontrar los componentes principales del Sistema de Gestión de Seguridad de la Información en la Entidad.

- **Estructura Organizacional de Seguridad de la Información:**

El Comité Institucional de Gestión y Desempeño del cual hace parte el Comité de Sistemas y Seguridad de la Información, es responsable de la dirección estratégica del Sistema de Gestión de Seguridad de la Información. El oficial o encargado de seguridad de la información y el proceso de gestión de la información y recursos tecnológicos son los responsables de la gestión del sistema, y un conjunto de responsabilidades separadas entre las áreas usuarias para el apropiado apoyo a la gestión de la seguridad de la información en la entidad.

- **Clasificación de Información:**

Desde el proceso de Gestión de Seguridad de la Información y Recursos Tecnológicos se realizó la adopción del instructivo para la clasificación de los activos de información

(PA03-IN), el cual proporciona los niveles de clasificación de la información, el formato para establecer el inventario de activos de información, software, hardware y servicios (PA03-FO), los cuales fueron acordados y socializados en sesiones con las diferentes áreas del Instituto para la Economía Social – IPES.

- **Políticas y Procedimientos de la Gestión de Seguridad:**

El MANUAL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PA03-MN) describe las políticas que soportan el SGSI y que se establecen para alcanzar niveles apropiados de seguridad de los activos de información del Instituto para la Economía Social – IPES.

- **Controles:**

Los controles determinados para implementar y la justificación de su selección o no, se encuentran descritos en la declaración de aplicabilidad, los cuales se encuentran alineados con la norma NTC-ISO-IEC 27001:2013 contiene:

- **Gestión del recurso humano:**

En el marco de las acciones del Comité Institucional de Gestión y Desempeño (resolución 564 de 2018) del Instituto para la Economía Social – IPES debe definir los roles y responsabilidades recomendados por los diferentes estándares de gestión de la seguridad de la información para los encargados de seguridad de la información, debe garantizar una socialización y concientización a todo el personal de la entidad en el conocimiento de las amenazas y responsabilidades por salvaguardar la confidencialidad, integridad y disponibilidad de la información.

- **Monitoreo y revisión de la gestión de seguridad:**

La entidad cuenta con un Sistema Integrado de Gestión (SIG) que considera los componentes para el seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información. Se debe fortalecer el esquema de control de registros de auditoría de los diferentes sistemas de información, así como la gestión y monitoreo centralizado de los activos de infraestructura tecnológica.

9.2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

9.2.1. Política General del Sistema de Gestión de Seguridad de la Información

La Dirección del Instituto para la Economía Social – IPES, consciente del crecimiento de los riesgos de seguridad digital, derivados del uso y masificación de las tecnologías de información y comunicaciones, considerando que la información es un activo esencial para la toma de decisiones encaminadas al cumplimiento de su misionalidad, se compromete a definir, implementar, mantener y mejorar un sistema de gestión de seguridad de la información que le permita contar con niveles apropiados de integridad, confidencialidad y disponibilidad de sus activos de información, en el marco del cumplimiento de las leyes, decretos, normas y lineamientos del orden Distrital y Nacional.

El Instituto para la Economía Social gestiona, a través del Comité Institucional de Gestión y Desempeño, los recursos necesarios para minimizar el impacto sobre los activos de información, a partir de una adecuada gestión de riesgo, promoviendo el compromiso y participación del talento humano y la mejora continua para apropiar una

cultura de seguridad de la información en el marco de su misión y objetivos institucionales.
Es obligación de todos los funcionarios, contratistas y terceros con acceso autorizado a la infraestructura tecnológica, servicios de red, aplicaciones y a los activos de información institucional, dar estricto cumplimiento a la política de seguridad y privacidad de la información del Instituto para la Economía Social

9.2.2. Objetivos del Sistema de Gestión de Seguridad de la Información

- Establecer lineamientos, directrices, controles y en general la intención de la Dirección del Instituto para la Economía Social de consolidar el uso apropiado de los servicios de procesamiento de información, que permitan la protección de los activos de información institucional.
- Definir la responsabilidad en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la entidad, al Comité Sistemas y Seguridad de la Información.
- Orientar a los funcionarios, contratistas y terceros sobre la responsabilidad de uso y buen manejo de los activos de información y de la infraestructura tecnológica que soporta la operación informática de la entidad.
- Definir aspectos a ser tenidos en cuenta por la entidad, relacionados con el talento humano y su responsabilidad en el uso de la información institucional antes, durante y en la terminación del vínculo laboral.
- Establecer directrices para la protección física de los activos de infraestructura tecnológica de la entidad.
- Establecer responsabilidades, controles y lineamientos en procura de proteger los sistemas y servicios informáticos por medio de los cuales se procesa la información institucional, que garanticen la operación informática de la entidad.
- Fomentar la conciencia alrededor de la importancia en el aseguramiento de la información institucional, la cual debe ser adoptada como una cultura organizacional.

9.2.3. Alcance del Sistema de Gestión de Seguridad de la Información

El desarrollo de la presente política de seguridad y privacidad de la información, así como la definición, implementación, mantenimiento y mejora de los controles de seguridad informática cubren todos los activos de infraestructura tecnológica (servidores, equipos de cómputo, equipos de comunicaciones, entre otros) y a todos los activos de información, (Bases de Datos, Documentos, SIG, Servicios Informáticos, documentos, registros), a fin de proteger la información institucional digital contra daño, pérdida, sustracción, modificación accidental o intencional, describiendo buenas prácticas en el uso de los sistemas y servicios informáticos, así como de los activos de tecnologías de información y comunicaciones, dispuestos por el Instituto para la Economía Social a los usuarios para el cumplimiento de sus funciones.

9.2.4. Plan de implementación del MSPI

La implementación del plan del Modelo de Seguridad y Privacidad de la Información comprende las siguientes actividades:

Actividades	Tareas	Responsable	INDICADOR	META	PRODUCTO	Fecha	
1. DIAGNÓSTICO ESTADO ACTUAL MSPI							
Determinar estado actual del MSPI	• Revisión de información actual. • Diligenciamiento del instrumento de diagnóstico de MSPI del MinTIC.	Profesional Seguridad de la Información-SDAE-	Documento instrumento de diagnóstico de MSPI del MinTIC actualizado	2	• Reporte de Revisión de información actual. • Instrumento de diagnóstico de MSPI del MinTIC.	01/02/2024 Y del 28/12/2024	28/02/2024 Y del 05/01/2025
2. GESTIÓN DE ACTIVOS DE INFORMACIÓN							
Lineamientos para la gestión de activos de información	• Revisión del instructivo de clasificación de activos de información. • Nota: De conformidad con el análisis sobre el instructivo, se determinará la necesidad de realizar actualización o no al instructivo	Subdirección de Diseño y Análisis Estratégico	Número de instructivo actualizado	1	• Acta de revisión o Instructivo de clasificación de activos de información actualizado (Según aplique)	01/03/2024	01/04/2024
Levantamientos activos de información	• Socialización de la documentación para la gestión de activos. • Actualización de inventarios de activos de información existentes. • Elaboración de inventario de activos para procesos misionales.	Profesional Seguridad de la Información-SDAE- Líderes de procesos	Inventarios de activos de información existentes realizados / programados	100	• Inventarios de activos de información , por HARDWARE, SOFWARE Y SERVICIO actualizado	16/06/2024	29/09/2024
Publicación de activos de información	• Consolidar los inventarios de activos de información. • Publicar los inventarios de activos de información.	Profesional Seguridad de la Información-SDAE-	Publicación de activos de información realizados/ programados	100	Publicación de activos de información	10/10/2024	15/11/2024
Registro de activos de información según Ley	• Actualizar el instrumento de	Profesionales -SDAE- Profesional Gestión	Número de Publicación del		Publicación del instrumento de registro		

Actividades	Tareas	Responsable	INDICADOR	META	PRODUCTO	Fecha	
1712 de 2014	registro de activos de Información. • Revisar viabilidad jurídica del instrumento para publicación. • Publicación del instrumento de registro de activos de información.	Documental -SAF-	instrumento de registro de activos de información realizado según Ley 1712 de 2014	1	de activos de información realizado según Ley 1712 de 2014	30/09/2024	02/10/2024
Reporte de bases de datos personales	• Reportar al área encargada las bases de datos personales Identificadas en el inventario de activos de información.	Profesional Seguridad de la Información- SDAE-	Reporte de Base de datos personales generadas	1	Reporte de Base de datos personales generadas	20/09/2024	20/10/2024
3. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL							
Revisión y Actualización de los lineamientos para la administración del riesgo.	• Revisión y/o actualización de la política de administración del riesgo. • Revisión y/o Actualización de la metodología para la gestión del riesgo. • Actualización de Formato Mapa de Riesgos. Nota: Inicialmente la entidad procederá a realizar la revisión si la metodología vigente requiere o no cambios de conformidad con la normatividad vigente o cambios en la administración del IPES	Subdirección de Diseño y Análisis Estratégico	Número documentos estratégicos de lineamientos para la administración del riesgo actualizada	3	• Revisión Política de Administración del riesgo publicada. • Metodología para la gestión del riesgo publicada • Formato Mapa de Riesgos publicada	01/03/2024	15/12/2024
Plan de formación Capacitación y sensibilización	• Socialización y entrenamiento a los encargados sobre el proceso de administración de Riesgos de seguridad digital.	Profesional en Seguridad de la Información - SDAE	Porcentaje de implementación del plan de formación y sensibilización	100%	• Plan de formación Capacitación y sensibilización	22/02/2024	22/11/2024
Proceso de administración de riesgos de seguridad digital.	• Identificación del riesgo. • Análisis del riesgo inherente. • Evaluación del riego inherente. • Definición de controles existentes. • Análisis del riesgo residual. • Selección de la opción de	Líderes de procesos	Porcentaje de implementación del Proceso de administración de riesgos de seguridad digital	3	• Matriz de riesgo corrupción del proceso	01/03/2023	15/12/2024

Actividades	Tareas	Responsable	INDICADOR	META	PRODUCTO	Fecha	
	tratamiento del riesgo. • Definición del plan de tratamiento. • Realimentación, revisión y verificación de los riesgos identificados (Ajustes).						
Aceptación de los riesgos residuales y aprobación del plan de tratamiento.	• Generar documento con la aceptación de los riesgos residuales y documento con la aprobación del plan del Tratamiento.	Líderes de procesos	Número de aceptaciones de los riesgos residuales y aprobación del plan de tratamiento	Por demanda	• Documento con la aceptación de los riesgos residuales y documento con la aprobación del plan del Tratamiento de riesgo.	18/04/2024	30/08/2024
Comunicación del riesgo.	• Presentar a las partes interesadas los resultados del proceso de administración o gestión del riesgo.	Profesional en Seguridad de la Información - SDAE Y SIG-MIPG	Número de Comunicación del riesgo generados	Por demanda	• Reportes de resultados del proceso de Administración o gestión del riesgo.	01/05/2024	15/05/2024
Seguimiento al plan de comités.	• Realizar seguimiento al estado de implementación de los comités y verificación de evidencias.	Profesional en Seguridad de la Información - SDAE Y SIG-MIPG	Porcentaje de efectividad de los comités	2	• Informe o reporte de los comités de sistemas y seguridad de la información que se realizan	13/06/2024	19/12/2204
Evaluación de la efectividad de los controles.	• Evaluación de riesgos incidentes de seguridad	Profesional en Seguridad de la Información - SDAE Y equipo SIG-MIPG	Número de evaluaciones de riesgos residuales realizadas sobre las programadas	Por demanda	• Reporte de Evaluación de riesgos o casos de incidentes de seguridad	02/02/2024	31/12/2024
Mejora continua.	• Identificación de las oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan de tratamiento.	Profesional en Seguridad de la Información - SDAE Y equipo SIG-MIPG	Número de Oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan	Por demanda	• Oportunidades de mejora continua acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan De tratamiento generados.	02/12/2024	31/12/2024

Actividades	Tareas	Responsable	INDICADOR	META	PRODUCTO	Fecha	
			de tratamiento				
Monitoreo y revisión.	• Generación, presentación y reporte de indicadores del plan de tratamiento.	Profesional en Seguridad de la Información y equipo SIG-MIPG	Número de Monitoreos y revisiones realizadas	Por demanda	• Reporte de indicadores del plan de tratamiento.	02/03/2024	31/12/2024
4. MARCO DOCUMENTAL							
Documentos Sistema de Gestión de la Seguridad de la Información	• Revisión y/o actualización de procedimientos asociados al Sistema de Gestión de la Seguridad de la Información	Equipo de gestión de seguridad de la información y recursos tecnológicos y Profesionales MIPG	Número de procedimientos revisados y/o actualizados	100%	• Acta de revisión y/o Procedimientos actualizados vigencia 2023 (Según aplique)	05/03/2024	30/11/2024
Políticas y manuales	• Revisión y actualización de políticas y manuales asociados al Sistema de Gestión de la Seguridad de la Información	Equipo de gestión de seguridad de la información y recursos tecnológicos y Profesionales MIPG	Número de políticas y manuales revisados y/o actualizados	100%	• Acta de revisión y/o Políticas y Manuales actualizados vigencia 2023 (Según aplique)	01/05/2024	31/12/2024
Declaración de aplicabilidad	• Revisión y actualización de declaración de aplicabilidad.	Profesional en Seguridad de la Información – SDAE	Número de Declaración de aplicabilidad actualizado	1	• Declaración de aplicabilidad	16/05/2024	20/12/2024
Normograma de seguridad de la información	• Identificación de la legislación aplicable. • Actualización de normograma de seguridad de la información. • Verificación del cumplimiento de los requisitos legales de seguridad de la información.	Profesional en Seguridad de la Información – SDAE Equipo gestión de seguridad de la información y recursos tecnológicos	normograma de seguridad de la información actualizado	1	• Documento de normograma de seguridad de la información actualizado	13/07/2024	20/09/2024
5. PLAN DE SENSIBILIZACION							
Plan de comunicación, sensibilización y capacitación para la entidad	• Ejecución de plan de plan de comunicación, sensibilización y capacitación. • Ejecución de pruebas de ingeniería social.	Profesional en Seguridad de la Información – SDAE Equipo gestión de seguridad de la información y recursos	Porcentaje de ejecución del Plan de comunicación, sensibilización y capacitación	100%	• Informe de ejecución del plan de comunicación, sensibilización	01/02/2024	29/12/2024

Actividades	Tareas	Responsable	INDICADOR	META	PRODUCTO	Fecha	
6. EVALUACION DEL DESEMPENO							
Indicadores de desempeño y eficacia SGSI	• Revisión y actualización de las métricas de los 2 planes de seguridad de la información y plan de tratamiento decreto 612 -2018	Profesional en Seguridad de la Información – SDAE Equipo gestión de seguridad de la información y recursos	Porcentaje de Revisión y actualización de las métricas de seguridad de la información	4	• Reportes de Revisión y actualización de las métricas de seguridad de la información	01/03/2024	18/12/2024
Revisión de la seguridad de la información	• Revisión independiente de la seguridad de la información. • Verificación del cumplimiento de las políticas y normas de seguridad.	Gestión de la seguridad de la información	Porcentaje de cumplimiento de la Revisión de la seguridad de la información ejecutada/ programada	1	• Revisión y actualización del Manual sistema de Gestión de Seguridad y Privacidad de la Información • Lista de chequeo eficiencia de los procedimientos de Verificación del cumplimiento de las políticas y normas de seguridad	06/15/2024	28/12/2024
7. MEJORA CONTINUA							
Acciones correctivas y de mejora	• Definición del plan de mejoramiento. • Ejecución de las acciones correctivas y de mejora. • Diagnóstico de Seguimiento al plande mejoramiento MSPI	Equipo gestión de seguridad de la información y recursos	Porcentaje de cumplimiento del Plan de Mejoramiento	1	• Diagnostico final de Seguimiento al plan de mejoramiento al MSPI	24/10/2024	31/12/2024

Tabla 1. Plan de implementación MSPI

10. MARCO NORMATIVO

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. 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.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC – Se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- 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 1952 de 2019. Por medio de la cual se expide el código general disciplinario
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 del 2012. Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Decreto compilado en el Decreto Único Reglamentario del sector Industria, Comercio y Turismo 1074 de 2015.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 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 relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1008 del 2018. 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.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.
- ISO/IEC 27001:2013 Information Technology Security Techniques – Information Security Management Systems- Requirements.
- ISO/IEC 27002 (Information Technology Security Techniques- odeo f Practice for Information Security Management.

11. DOCUMENTOS ASOCIADOS

- PA03-PD-005 V2 Trabajo en Áreas Seguras
- PA03-PD-010 V2 Control de Cambios
- PA08-PD-003 V3 Gestión de Usuarios
- PA03-PD-006 V2 Instalación de Software en Sistemas Operativos
- PA08-PD-005 V3 Transferencia de Información
- PA03-PD-011 V2 Implementación de la Continuidad de la Seguridad de la Información
- PA03-PD-007 V2 Gestión de Medios Removibles y Disposición de los Medios
- PA03-PD-002 V5 Gestión de Incidentes de Seguridad de la Información
- PA03-PD-001 V5 Atención Mesa de Ayuda
- PA03-IN Gestión De Incidentes De Seguridad
- PA03-IN Clasificación de activos de información
- PA03-MN-001 V4 Sistema de Gestión de Seguridad y Privacidad de la Información
- PA03-MN-002 V2 Manual Usuario Herramienta Misional HEMI
- PA03-MN-003 V2 Manual Técnico Herramienta Misional HEMI
- PL-21 POLITICA PARA EL TRATAMIENTO DE DATOS PERSONALES

12. ANEXOS

Sin anexos.

13. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
1	30/07/2018		Elaboración del documento
2	21/01/2019		Se ajustó al formato FO-697
3	10/01/2020	Responsabilidades	Se incluye la descripción de los roles y responsabilidadesde seguridad y privacidad de la información en la entidad.
		Marco Normativo	Se incluye y se actualiza el Marco Normativo que aplica
4	20/01/2021	Todos	Actualización de todos los Numerales del plan.
5	18/01/2022	Responsabilidades Plan de Implementación Del MSPI Documentos asociados	Actualización de los textos
6	20/02/2024	Responsabilidades Plan de Implementación Del MSPI Documentos asociados	Actualización de los textos