ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital de las Artes

GUÍA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

BOGOTÁ | INSTITUTO DISTRITAL DE LAS ARTES IDARTES

HISTÓRICO DE CAMBIOS		
Versión	**Fecha de emisión**	**Cambios realizados**
1	22/05/2024	Emisión inicial

Elaboró	Revisó	Aprobó	Avaló
Maryury Forero Bohórquez Contratista Oficina Asesora de Planeación y Tecnologías de la Información	**Jonathan González** Profesional Universitario Oficina Asesora de Planeación y Tecnologías de la Información	**Daniel Sánchez Rojas** Jefe Oficina Asesora de Planeación y Tecnologías de la Información	**Daniel Sánchez Rojas** Jefe Oficina Asesora de Planeación y Tecnologías de la Información
Astrid Jaramillo Betancur Contratista Oficina Asesora de Planeación y Tecnologías de la Información	**María Cristina Herrera Calderón** Contratista Oficina Asesora de Planeación y Tecnologías de la Información		

TABLA DE CONTENIDO

1. INTRODUCCIÓN 6

2. OBJETIVOS 6

2.2 Objetivos Específicos 6

3. GENERALIDADES 7

3.1 Sistema de Seguridad de la Información - SGSI 7

3.2 Para qué sirve el SGSI 7

3.3 DEFINICIONES 7

4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 8

4.1 Marco Normativo 9

4.2 Políticas de Seguridad de la Información 10

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 10

5.1. Estructura de lineamientos SGSI 10

6. ORGANIZACIÓN DE SEGURIDAD 12

7. RESPONSABILDIADES Y ROLES 12

7.1 Comité Directivo 12

7.2 Oficial de Seguridad de la Información 13

7.3 Directores, subdirectores, gerentes, asesores y jefes de oficina 13

7.5 Uso, apropiación y divulgación 14

7.6 Revisión del SGSI 14

8. RIESGOS 14

8.1 Determinar los riegos 14

8.2 Valoración del riesgo 15

9. DECLARACIÓN DE APLICABILIDAD SOA 15

10. DISEÑO DEL SGSI 16

11. REVISIÓN DEL SGSI 17

12. MEJORA DEL SGSI 17

Tabla de Ilustraciones

Ilustración 2. Ciclo PHVA-elaboración propia..... 11
Ilustración 3. Análisis de riesgos – elaboración propia..... 15

Tabla de Tablas

Tabla 1. Fases del ciclo PHVA – elaboración propia..... 11
Tabla 2.Resumen de la Información Documentada para el SGSI 16

1. INTRODUCCIÓN

Establecer una guía del Sistema de Gestión de Seguridad de la Información -SGSI, permitirá al IDARTES la implementación de los controles administrativos y técnicos necesarios para garantizar y asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información, dando cumplimiento a la Norma NTC-ISO- IEC27001 y los lineamientos dados por la Alta Consejería Distrital para las TIC establecidos en la Política Nacional de Seguridad Digital y Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC, contenida en el documento CONPES 3854 de abril de 2016 y adoptando el Modelo de Seguridad y Privacidad de la Información – MSPI, el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad de la Información, que se encuentra alineado con el Marco de Referencia de Arquitectura de TI del Plan Estratégico de Tecnologías de la Información-PETI.

La guía del Sistema de Gestión de Seguridad de la Información proporciona directrices fundamentales para el diagnóstico, planificación, implementación, gestión y mejora continua del Sistema de Gestión de Seguridad de la Información. Este documento cuenta con las necesidades y objetivos específicos, los requisitos de seguridad, los procesos que involucran la manipulación de información, así como los responsables y roles dentro del IDARTES.

2. OBJETIVOS

2.1 Objetivo General

Definir los procesos, controles y las directrices principales en relación a la seguridad y privacidad de la información y el mantenimiento del SGSI enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar) para la implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información-MSPI.

2.2 Objetivos Específicos

- Definir el alcance, objetivos, responsabilidades y las directrices principales en relación con seguridad de la información, mantenimiento y mejora del SGSI enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).
- Contribuir con la seguridad de la información producida, procesada y gestionada por las Unidades de gestión del IDARTES.
- Identificar y gestionar los riesgos de seguridad y privacidad de la información a niveles aceptables.

3. GENERALIDADES

3.1 Sistema de Seguridad de la Información - SGSI

El Sistema de Gestión de Seguridad de la Información permite mantener la confidencialidad, integridad, disponibilidad y privacidad de la Información.

- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Siendo un atributo que debe tener la información, para que sea divulgada únicamente por personas o entidades autorizadas por el IDARTES, en el momento que se requiera.

- **Integridad:** La información y sus métodos de procesamiento se mantienen con exactitud y completitud. Siendo un atributo que deben tener los datos o la información, para que no sean alterados ni destruidos por personas o entidades no autorizadas por el IDARTES.

- **Disponibilidad:** Acceso y utilización de la información y de los sistemas de tratamiento, por parte de los individuos, entidades o procesos autorizados, cuando lo requieran. Siendo un atributo que deben tener los datos o la información, para que sean consultados y tratados por personas o entidades autorizadas por el IDARTES, con oportunidad.

3.2 Para qué sirve el SGSI

El Sistema de Gestión de Seguridad de la Información establece políticas y procedimientos con el fin de minimizar los siguientes factores que pueden afectar la información y la continuidad de los procesos, objetivos estratégicos, misión y visión del IDARTES:

- **Vulnerabilidad:** Todas aquellas fallas, omisiones, o deficiencias de seguridad que pueden ser aprovechadas por cualquier individuo para poner en riesgo la información o la continuidad del negocio.

- **Riesgo:** Probabilidad de que se materialice la amenaza.

- **Amenaza:** Es la posibilidad de que un sistema vulnerable sea atacado y sufra daños.

3.3 DEFINICIONES

- **Activo (Asset):** Cualquier cosa que tiene valor para la entidad, la norma ISO/IEC 27000, define los siguientes tipos de activos: información; software, hardware, servicios, personas.
- **Activo de información:** Conocimiento o información que tiene valor para el IDARTES.
- **Antivirus:** Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.
- **Autorización:** Proceso de definir los derechos o permisos asignados a un usuario.
- **Cifrado:** Método que permite aumentar la seguridad de la información mediante la codificación, de manera que solo pueda leerlo la persona que tenga la clave de cifrado adecuada para

descodificarlo.

- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones**.**
- **Control**: En seguridad de la Información se pueden definir como controles, las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para llevar y mantener los riesgos de Seguridad de la Información por debajo del nivel de riesgo asumido.
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el sistema de gestión de la seguridad de la información (SGSI), 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 la norma técnica NTC-ISO/IEC 27001:2013.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona/entidad autorizada. la información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, entre otros.) dentro del alcance del SGSI, que tengan valor para IDARTES y necesiten por tanto ser protegidos de potenciales riesgos**.**
- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la seguridad de la información.
- **Incidente de seguridad informático:** Violación o amenaza que afecta la confidencialidad, integridad y disponibilidad, como la continuidad de los servicios ofrecidos por el IDARTES.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud, la información debe ser de calidad, clara y completa, y solo podrá ser modificada por el personal expresamente autorizado para ello, la falta de integridad de la información puede exponer a la entidad a toma de decisiones incorrectas, lo cual puede tener impacto reputacional, financiero y legal.
- **Propiedad Intelectual:** Incluye patentes, marcas registradas, derechos de autor y secretos comerciales.
- **Seguridad de la información:** Preservación de los principios de confidencialidad, la integridad y la disponibilidad de la información.
- **Sistema de gestión de la seguridad de la información:** Conjunto de elementos interrelacionados o interactuantes (políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza la entidad para establecer la política y los objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La seguridad y privacidad de la información aplica a todo el recurso humano interno y externo (funcionarios, contratistas, proveedores, pasantes, entre otros) del IDARTES, y a terceros o externos que por el cumplimiento de sus funciones y las del IDARTES compartan, utilicen, recolecten, procesen, intercambien, transformen o consulten información, así como los entes de control, entidades relacionadas que accedan, ya sea interna o externamente, a cualquier tipo de información física o digital, independientemente de su ubicación. Así mismo, esta guía del SGSI aplica a toda la información creada, procesada o utilizada por el IDARTES, sin importar el medio, formato, presentación o lugar en

el cual se encuentre.

El alcance inicial preliminar del SGSI comprende la política de seguridad de la información, los procedimientos y controles establecidos en el MSPI para mantener los pilares de la información Confidencialidad, Integridad y Disponibilidad transmitida y procesado por funcionarios del IDARTES, enfocado en la Norma NTC-ISO-IEC 27001.

Las limitaciones para la implementación del SGSI son las siguientes:

Se relacionan a continuación algunas dificultades que podrían limitar la implementación del SGSI:

- Disponibilidad de tiempo
- Recursos económicos
- Renovación de software y hardware
- Gestión del cambio
- Cambio continuo del personal a cargo
- Identificar los activos de información importantes
- Aplicaciones, redes, recursos de TI
- Requisitos legales y reglamentarios
- Conciencia sobre la seguridad de la información

4.1 Marco Normativo

- *Decreto 1008 de 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".

- *Decreto 1080 de 2015:* 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.

- *Ley 1712 de 2014:* (Ver Ley 2199 de 2022). 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 Estatutaria 1581 de 2012:* Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022.

- Ley Estatutaria por la cual se reglamenta el artículo 15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales.

- *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 527 de 1999:* Desarrollado por el Decreto 4487 de 2009 - Reglamentado parcialmente por el Decreto 1747 de 2000. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información.

Políticas de Seguridad de la Información

- Las directrices del Sistema de Gestión de Seguridad de la Información son de aplicación obligatoria para todo el personal, sin importar el nivel jerárquico o su posición en el organigrama de la entidad y se establecen en la Política de Seguridad y Privacidad de la Información. Para su aplicación, se deben tener en cuenta los siguientes objetivos:

- Definir las pautas, directrices y reglas para generar una adecuada seguridad y protección de la información de las unidades de gestión del IDARTES, estableciendo dentro del plan estratégico de la OAPTI su liderazgo y desarrollo.

- Informar al mayor nivel de detalle, a los usuarios, directivos, funcionarios, contratistas y terceros las normas y mecanismos que deben cumplir en las interacciones con los activos de información del IDARTES, y establecer el alcance de las responsabilidades que compromete en la gestión a cada uno de ellos.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1. Estructura de lineamientos SGSI

La Norma ISO27001, adapta una serie de lineamientos para la implementación del sistema de Gestión de Seguridad de la Información, los cuales se pueden alinear con otros sistemas de gestión en IDARTES; la estructura se establece de la siguiente forma:

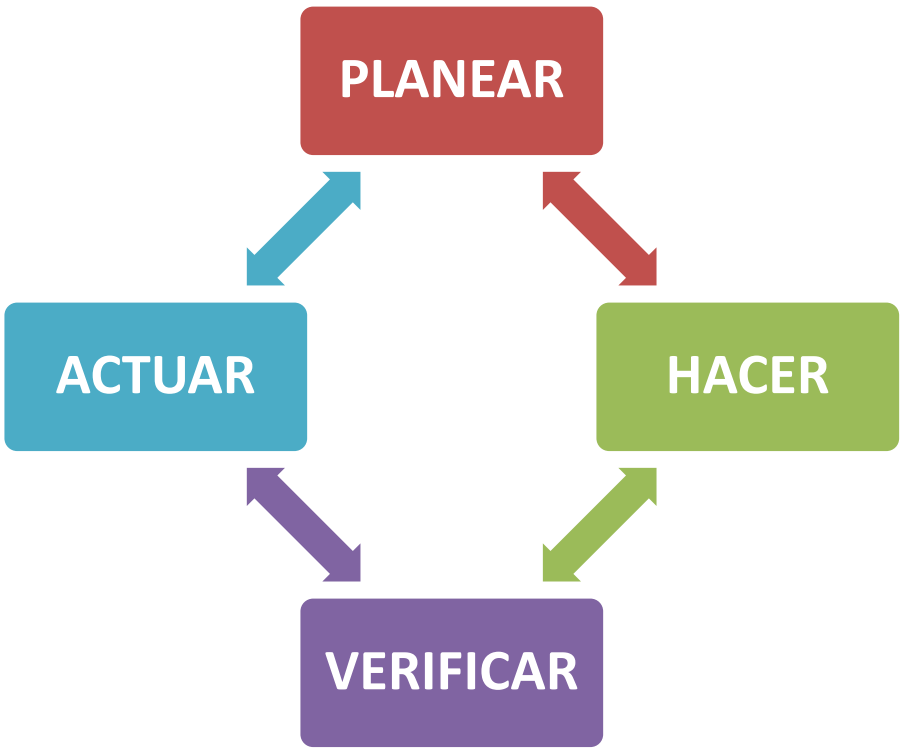

Ilustración 1. Ciclo PHVA.
Fuente. Elaboración propia

A continuación, se describen los componentes de cada una de estas fases del ciclo PHVA:

Tabla 1. Fases del ciclo PHVA para el SGSI

Planear – Establecer el SGSI	Hacer – Implementar y establecer el SGSI
✓ Definir el alcance. ✓ Generalidades. ✓ Análisis de riesgos. ✓ Selección de controles. ✓ Plan de Seguridad y Privacidad de la Información. ✓ Aceptación de los riesgos residuales. ✓ Aplicar la matriz Declaración de Aplicabilidad de la Norma ISO 27001:2013	✓ Actividades Plan de Seguridad y Privacidad de la Información. ✓ Actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. ✓ Implementación de la estrategia de uso y apropiación TI. ✓ Gestión de la operación. ✓ Gestión de incidentes de seguridad de la información. ✓ Aplicación del modelo de seguridad y privacidad de la información del MINTIC.
Verificar – Monitorear el SGSI	**Actuar – Mantener y mejorar el SGSI**

Planear – Establecer el SGSI	Hacer – Implementar y establecer el SGSI
✓ Revisar la eficacia del SGSI. ✓ Auditorías internas y externas. ✓ Actualizar Plan de Seguridad y Privacidad de la Información. ✓ Actualizar Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. ✓ Declaración de Aplicabilidad de la Norma ISO 27001:2013	✓ Implementar mejoras. ✓ Aplicar medidas correctivas y preventivas ✓ Comunicar las acciones. ✓ Asegurar el cumplimiento de objetivos.

Fuente. Elaboración propia

6. ORGANIZACIÓN DE SEGURIDAD

Dentro del IDARTES, se ha adoptado e implementado un conjunto integral de medidas para garantizar la seguridad y privacidad de la información. Estas incluyen, la implementación del Plan de Seguridad y Privacidad de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Modelo de Seguridad y Privacidad de la Información -MSPI y la Política de Seguridad y Privacidad de la Información. Estos documentos establecen acciones específicas destinadas a salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Además, se cuenta con un profesional que ejecuta el rol de Oficial de Seguridad de la Información, quien tiene la responsabilidad de ejecutar estas acciones. Dentro de sus obligaciones se incluye la gestión proactiva de riesgos, la implementación de controles de seguridad y la promoción de una cultura de protección de la información dentro del IDARTES.

7. RESPONSABILDIADES Y ROLES

A continuación, se definen las responsabilidades de los funcionarios, contratistas, y partes interesadas del IDARTES frente al Sistema de Gestión de Seguridad de la Información-SGSI.

7.1 Comité Directivo

Es parte fundamental en la implementación de un SGSI, el seguimiento y su mejora continua; el apoyo del CIGD del IDARTES es de suma importancia, ya que repercute directamente en el cumplimiento de la misión de la entidad.

Algunas de las actividades efectuadas por el Comité Directivo son:

- Comunicar a la entidad tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.
- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.

- Aprobar el Plan de Seguridad y Privacidad de la Información, el Plan de Implementación del Sistema General de Seguridad de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y demás documentación relacionada con el SGSI.

7.2 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información del IDARTES, hace parte de la Oficina Asesora de Planeación y Tecnologías de la Información y es responsable del diseño, desarrollo, implementación, mantenimiento y verificación del correcto funcionamiento del Sistema de Gestión de Seguridad de la Información-SGSI, articulado con los requerimientos normativos vigentes del Ministerio de las TIC y la Alta Consejería Distrital de TIC, el cual tendrá las siguientes responsabilidades:

- Apoyar a las diferentes Unidades de Gestión del IDARTES en el análisis de riesgos de la información.
- Diseñar, desarrollar, establecer y controlar las acciones encaminadas a Seguridad y Privacidad de la Información.
- Establecer los lineamientos, documentación y buenas prácticas de seguridad y privacidad de la información.
- Definir la arquitectura de seguridad de información en línea con la arquitectura de tecnología de la Entidad.
- Determinar e implementar la estrategia de uso y apropiación de seguridad y privacidad de la información.
- Establecer indicadores de gestión de seguridad y privacidad de la información en la Entidad.
- Asesorar en materia de seguridad y privacidad de la información a la Entidad.
- Promover el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en el IDARTES.
- Gestionar los incidentes de seguridad y privacidad de la información reportados e identificados por los funcionarios/contratistas o terceros.

7.3 Directores, subdirectores, gerentes, asesores y jefes de oficina

a) Estos roles deben asegurar que todos los procedimientos de seguridad y privacidad de la información se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información en el IDARTES.

b) Los responsables de la información en el IDARTES deben valorarla, identificar los riesgos a que se expone y velar por que se apliquen los mecanismos necesarios para mitigar los riesgos a niveles aceptables. Frente a las responsabilidades de seguridad y privacidad de la información, estas son algunas de ellas:

- Identificar los activos, riesgos y controles para el manejo de la información.
- Apoyar al Oficial de Seguridad y Privacidad de la Información en la identificación de los requerimientos de seguridad de la información.
- Participar en las auditorias del Sistema de Gestión de Seguridad de la Información.
- Solicitar los accesos a los sistemas de información sobre los cuales sean responsables de acuerdo con los lineamientos definidos por la Oficina Asesora de Planeación y

Tecnologías de la Información-OAPTI.

7.5 Uso, apropiación y divulgación

El uso, la apropiación y la divulgación del SGSI son fundamentales para su efectividad en el IDARTES, algunas de las actividades que se desarrollarán son:

- Comunicaciones masivas de información
- Capacitaciones, charlas, sensibilizaciones, entre otras, por parte de la OAPTI.
- Correos masivos con piezas informativas relacionadas con seguridad y privacidad de la información.

7.6 Revisión del SGSI

La revisión del SGSI busca asegurar que sus objetivos se estén logrando y que continúen siendo adecuados y efectivos.

- Auditorías internas y/o externas.
- Informes de estado de las acciones correctivas y preventivas.
- Recomendaciones de mejora.
- Cambios que afecten al SGSI.
- Gestión de riesgos de seguridad y privacidad de la información.
- Actualización planes estratégicos del Decreto 612 de 2018.
- Identificación y/o actualización de activos de información.

8. RIESGOS

8.1 Determinar los riegos

Durante esta fase, es crucial llevar a cabo un exhaustivo estudio preliminar destinado a identificar los riesgos, vulnerabilidades y amenazas que puedan afectar a varios sistemas en operación dentro del IDARTES. Estos sistemas abarcan desde los servidores hasta la red LAN, WAN, WIFI, pasando por las estaciones de trabajo, el software y los sistemas de información. Este análisis detallado proporcionará una base sólida para diseñar estrategias efectivas de mitigación de riesgos y garantizar la seguridad integral de los activos de información del IDARTES.

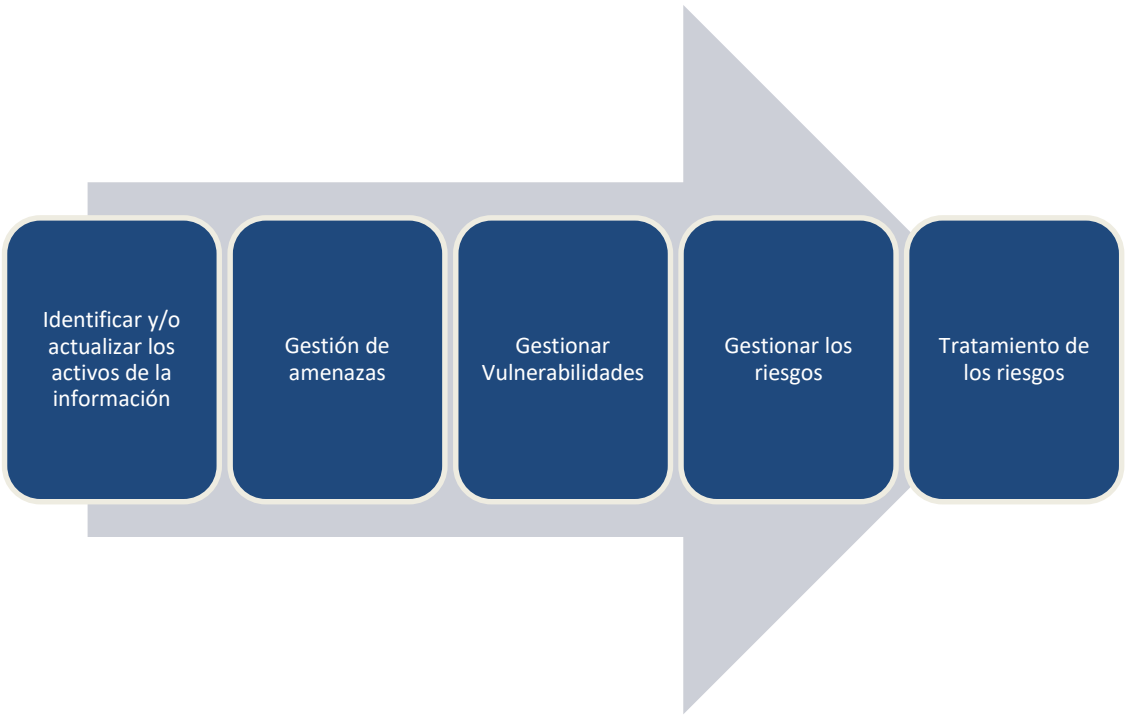

Ilustración 2. Análisis de riesgos
Fuente. Elaboración propia

8.2 Valoración del riesgo

La valoración del riesgo constituye el eje principal del Sistema de Gestión de Seguridad de la Información (SGSI). En este proceso es crucial considerar los parámetros de probabilidad de ocurrencia, los parámetros de impacto, la vulnerabilidad y los criterios de aceptación del riesgo.

Para el sistema de Gestión de la Información – SGSI, la OAPTI, maneja tres grandes atributos de información, **confidencialidad, integridad y disponibilidad**.

9. DECLARACIÓN DE APLICABILIDAD DE LA NORMA ISO 27001:2013

Documento que enlista los controles de seguridad establecidos en el anexo “A” de la Norma ISO 27001, los cuales son contemplados por el SGSI a través de la implementación del MSPI adoptado por el IDARTES a través del formato GTI-F-21- GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

El IDARTES a través de la OAPTI, es la responsable de implementar, operar, mantener y mejorar el SGSI, lo cual permite garantizar el funcionamiento, la continuidad y seguridad del negocio.

La Declaración de Aplicabilidad será revisada de acuerdo con los resultados obtenidos en la valoración de riesgos y/o cambios significativos de los elementos de la plataforma tecnológica y en los periodos convenidos para su actualización.

10. DISEÑO DEL SGSI

Un Sistema de Gestión de Seguridad de la Información-SGSI, radica en el diseño, la implementación y el mantenimiento de un conjunto de procesos destinados a gestionar de manera eficiente la accesibilidad de la información. Este enfoque tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de los activos de información, al mismo tiempo que se minimicen los riesgos de seguridad. Mediante la aplicación de medidas y controles adecuados a través del Modelo de Seguridad y Privacidad de la Información-MSPI, el SGSI busca proteger los recursos de información del IDARTES y preservar su valor y utilidad para la entidad.

Tabla 2.Resumen de la Información Documentada para el SGSI

Numeral	ISO-TEC 27001	Documentación
4.3	Determinación del alcance del SGSI	Debe estar disponible como información documentada.
5.2	Política de Seguridad y Privacidad de la Información	Debe estar disponible como información documentada.
6.1.2	Valoración del riesgo de seguridad de la información	Información documentada acerca del proceso de gestión de los riesgos de seguridad de la información.
6.1.3	Tratamiento de riesgos de seguridad y privacidad de la información	Información documentada acerca del proceso de tratamiento de riesgos de seguridad y privacidad de la información.
6.1.3	Declaración de Aplicabilidad de la Norma ISO 27001:2013	Declaración de Aplicabilidad de la Norma ISO 27001:2013
6.2	Objetivos de seguridad de la información y planes para lograrlos	Debe estar disponible como información documentada.
7.2	Competencia	Debe estar disponible como información documentada.
7.5	Información documentada	La que la entidad determine que es necesaria para el SGSI.
7.5.3	Control de la información documentada	La información documentada de origen externo.
8.1	Planificación y control operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo con la planificación.
8.2	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información.

Numeral	ISO-TEC 27001	Documentación
9.1	Seguimiento, medición, análisis y evaluación.	Evidencia de los resultados del monitoreo y la revisión.
9.2	Auditoría interna	Conservar la información documentada como evidencia de la implementación del programa de auditoría y los resultados de esta.
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por el CIGD.
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada.
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva.

Fuente. Elaboración propia

11. REVISIÓN DEL SGSI

La OAPTI verificará el cumplimiento y el seguimiento a los compromisos derivados del SGSI, igualmente hará una revisión al año, donde se evalúan las oportunidades de mejora y la necesidad de realizar ajustes a la estructura del SGSI.

12. MEJORA DEL SGSI

A partir de los incidentes o situaciones de mejora identificados por diferentes fuentes, la OAPTI definirá la metodología a seguir para eliminar las causas de las no conformidades reales o potenciales con el objeto de evitar nuevamente su ocurrencia, dicha gestión finaliza con la validación, por parte de la OAPTI, de la efectividad de las acciones previstas en el plan de acción hasta su cierre.

Radicado: **20244300321253**
Fecha 22-05-2024 09:22

Documento 20244300321253 firmado electrónicamente por:

DANIEL SÁNCHEZ ROJAS, Jefe Oficina Asesora de Planeación y Tecnologías de la Información, Oficina Asesora de Planeación, Fecha de Firma: 22-05-2024 12:21:48

ASTRID JARAMILLO BETANCUR, Contratista, Oficina Asesora de Planeación, Fecha de Firma: 22-05-2024 11:00:36

MARYURY FORERO BOHORQUEZ, Contratista, Oficina Asesora de Planeación, Fecha de Firma: 22-05-2024 09:31:29

JONATHAN GONZÁLEZ BOLAÑOS, Profesional Universitario Código: 219 Grado: 01, Área de Tecnología, Fecha de Firma: 22-05-2024 10:12:43

MARIA CRISTINA HERRERA CALDERON, , Oficina Asesora de Planeación, Fecha de Firma: 22-05-2024 23:33:01

Revisó: SANDRA PATRICIA MORENO BOHORQUEZ - Técnico Administrativo - Área de Tecnología

b8c67a303b6f7c7f52cd437fa905bd4a5fbaba8518e45767633b3a927fe81a4f