
	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	Plan de Seguridad y Privacidad de la Información		
	Código:	Versión :03	Fecha de emisión: 2025
			Pagina 1

# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

## Modelo de Seguridad y Privacidad de la Información


IDEA

2024- 2027


	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD			
	Plan de Seguridad y Privacidad de la Información			
	Código:	Versión :03	Fecha de emisión: 2025	Pagina 2

## Tabla de contenido

<b>1.</b>	<b>INTRODUCCIÓN .....</b>	<b>4</b>
<b>2.</b>	<b>OBJETIVO.....</b>	<b>4</b>
<b>3.</b>	<b>DEFINICIONES .....</b>	<b>4</b>
<b>4.</b>	<b>DOCUMENTOS DE REFERENCIA .....</b>	<b>7</b>
<b>5.</b>	<b>CICLO DE OPERACIÓN.....</b>	<b>9</b>
<b>6.</b>	<b>Fase de Diagnóstico .....</b>	<b>9</b>
6.1	Instrumento de Evaluación ISO 27001:2022 y Ciberseguridad .....	10
6.1.1	Levantamiento de información .....	10
6.1.2	Desarrollo .....	10
6.1.3	Análisis de la Información.....	10
6.1.4	Resultados .....	10
<b>7.</b>	<b>Fase de Planificación.....</b>	<b>11</b>
7.1	Contexto .....	11
7.1.1	Comprensión de la organización y su contexto .....	11
7.1.2	Alcance .....	12
7.2	Liderazgo.....	12
7.2.1	Liderazgo y Compromiso .....	12
7.2.2	Política de Seguridad de la Información y Ciberseguridad .....	12
7.2.3	Roles y Responsabilidades .....	13
7.3	Planificación .....	13
7.3.1	Identificación de activos de información e infraestructura critica.....	13
7.3.2	Valoración de los riesgos de seguridad de la información .....	14
7.3.3	Gestión de Incidentes de Seguridad.....	14
7.4	Soporte .....	16
7.4.1	Recursos .....	16
7.4.2	Competencia, toma de conciencia y comunicación .....	16
<b>8.</b>	<b>Fase de Operación.....</b>	<b>16</b>

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión:</b> <b>2025</b>	<b>Pagina 3</b>

8.1	Planificación e implementación .....	17
<b>9.</b>	<b><i>Fase de Evaluación de Desempeño .....</i></b>	<b>20</b>
9.1	Seguimiento, medición, análisis y evaluación .....	21
9.2	Auditoría Interna .....	22
9.3	Revisión por la Dirección.....	22
<b>10.</b>	<b><i>Fase de Mejoramiento Continuo .....</i></b>	<b>22</b>
10.1	Mejora .....	22
<b>11.</b>	<b><i>Control de Cambios .....</i></b>	<b>23</b>

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 4</b>

## INTRODUCCIÓN

El presente documento brinda los lineamientos y orienta las actividades a desarrollarse durante el presente año para la adaptación del Instituto para el Desarrollo de Antioquia - IDEA al Modelo de Seguridad y Privacidad de la Información (MSPI) emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de conformidad con la política de gobierno digital, el Departamento Administrativo de la Función Pública y la norma técnica NTC ISO/IEC 27001:2022; a su vez que se integra con el programa de Protección de Datos Personales y La Gestión de Riesgos de Seguridad de la Información en el IDEA.

Para llevar a cabo la implementación del MSPI se debe contar con el Plan de Seguridad y Privacidad de la Información que se actualizará y publicará anualmente de conformidad con el Decreto 612 de 2018. En cumplimiento de la Ley 1581 de 2012, sus decretos reglamentarios y los lineamientos emitidos por la Superintendencia Financiera de Colombia, el presente modelo contempla la generación de un Programa Integral de Protección de Datos Personales, la preservación de la confidencialidad, integridad y disponibilidad de la información y la gestión de la continuidad de la operación


El Plan será revisado con regularidad, dando cumplimiento al Modelo Integrado de Planeación y Gestión -MIPG- Se deberá actualizar al identificar cambios en la normatividad en el negocio, en su estructura, objetivos o en general, para asegurar que se ajuste a los requerimientos identificados.

### 1. OBJETIVO

Definir el Plan de Seguridad y Privacidad de la Información MSPI en el IDEA con la finalidad de facilitar la implementación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad SGSI, aplicando lineamientos de buenas prácticas que permitan proteger los activos de seguridad de la información basados en el ciclo PHVA (Planear, Hacer, Verificar y Actuar) y de acuerdo con la norma NTC ISO/IEC 27001:2022.


### 2. DEFINICIONES

- ✓ Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas,


	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 5</b>

soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

- ✓ Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- ✓ Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- ✓ Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- ✓ Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- ✓ Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- ✓ Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- ✓ Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- ✓ Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- ✓ Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 6</b>

- ✓ Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
- ✓ Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- ✓ Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- ✓ Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- ✓ Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- ✓ Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- ✓ Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- ✓ Sistema de Gestión de Seguridad de la Información: SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- ✓ Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).


	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 7</b>

- ✓ Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- ✓ Partes interesadas (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

### **3. DOCUMENTOS DE REFERENCIA**


El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Circular Externa Conjunta No. 04 del 5 de septiembre de 2019 Tratamiento de datos personales en sistemas de información interoperables.
- Circular Externa 033 de 2020
- Circular Externa 005 de 2019
- Circular Externa 008 de 2018
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- 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 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- 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.
- 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 Único 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.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 8</b>

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital. • .
- 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.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario
- Decreto 612 de 2018, “*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. “*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*”.
- Manual de Gobierno Digital – MINTIC.



	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 9</b>

- Modelo de Seguridad y Privacidad de la Información – MINTIC.

#### 4. CICLO DE OPERACIÓN

El Modelo MSPI del IDEA toma como referencia el definido en el Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y Comunicaciones en su Versión 4, el cual está basado en el ciclo PHVA conforme al estándar internacional ISO/IEC 27001:2022; así como los requerimientos legales, técnicos, normativos, reglamentarios, de funcionamiento y necesidades y expectativas de las partes interesadas.

El modelo consta de cinco (5) fases las cuales se gestiona y se mantiene adecuadamente la seguridad de los activos de información.

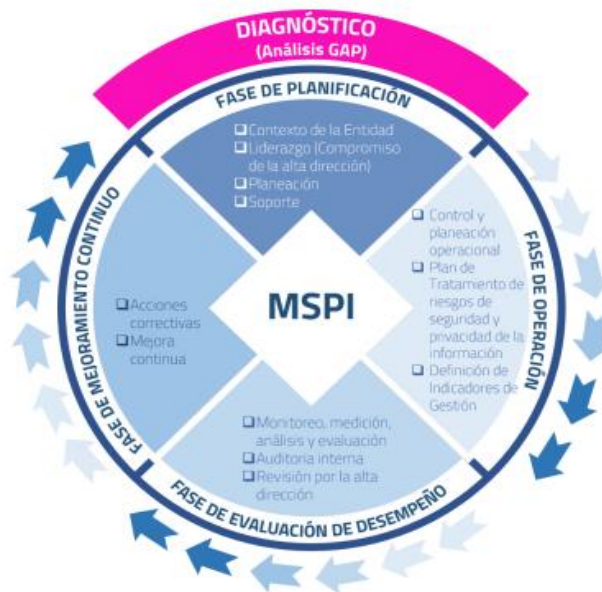



Figura 1 - Ciclo Modelo de Seguridad y Privacidad de la Información (Tomado MSPI - Min Tic V4)

#### 5. Fase de Diagnóstico

En esta fase se realiza un análisis del estado actual del IDEA respecto a la adopción del Modelo de Seguridad y Privacidad de la Información MSPI.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>		
	<b>Plan de Seguridad y Privacidad de la Información</b>		
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>
			<b>Pagina 10</b>

El IDEA realizó valoraciones de los controles del Anexo A, del Sistema de Gestión de Seguridad y Privacidad de la Información y de Ciberseguridad conforme al Instrumento de Evaluación de la ISO 27001-2022 y Ciberseguridad.

## **5.1 Instrumento de Evaluación ISO 27001:2022 y Ciberseguridad**

Este Instrumento, es la herramienta de diagnóstico para conocer el estado actual de la gestión de la seguridad y privacidad de la información en el Instituto, así como, el nivel de madurez de los controles de seguridad utilizados.

La ejecución de la evaluación se realizó en las siguientes fases:

### **5.1.1 Levantamiento de información**

Se identifica la información y datos existentes necesarios para realizar la evaluación.

### **5.1.2 Desarrollo**


Diligenciamiento de la herramienta elegida para la realización del diagnóstico e identificación de brechas en seguridad de la información.

### **5.1.3 Análisis de la Información**

- Pruebas Administrativas: Se recopila temas de seguridad de la información de las áreas que no están directamente relacionadas con las áreas tecnológicas del Instituto, así como Políticas de Seguridad, Responsabilidades, acuerdos de confidencialidad, necesidades y expectativas de las partes interesadas, cumplimiento de requisitos de seguridad de la información de los proveedores y el establecimiento del Plan de Continuidad del Negocio.
- Pruebas Técnicas: se evaluaron todos los requisitos de la Norma ISO 27001:2022, controles del Anexo A de la norma ISO 27001, requisitos de la Norma NIST, requisitos del Modelo de Seguridad y Privacidad de la Información de Mintic, Gobierno Digital y mejores prácticas de ciberseguridad.

### **5.1.4 Resultados**

- Brecha requisitos de la norma, Anexo ISO 27001:2022 y NIST:2018

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 11</b>

En este componente se muestra el resultado del análisis de brecha frente a los requisitos y controles del Anexo A, del estándar ISO 27001:2022, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la información.

- **Porcentaje de Cumplimiento**

Los criterios a tener en cuenta en la valoración de cada requisito y control con la finalidad de obtener un porcentaje de cumplimiento de los capítulos y anexo A de la Norma ISO 27001:2022 y requisitos de la Instituto Nacional de Estándares y Tecnología - NIST

NO APLICA= Marque con una “X”, Cuando se ha excluido el requisito y este no afecta la capacidad ni la responsabilidad para cumplir requisitos por parte de la organización.

COMPLETO= Marque con una “X”, en el caso de haber realizado TODAS las acciones requeridas, poseer evidencias suficientes y tener resultados eficaces de cumplimiento del requisito.

PARCIAL= Marque con una “X”, en el caso de no haber realizado al menos una acción o actividad requeridas, poseer evidencias insuficientes y a pesar de obtener resultados, estos no son eficaces.


NINGUNO= Marque con una “X”, en caso de no encontrar ninguna acción o actividad relacionada, no se poseen evidencias ni resultados relacionados con el requisito.

## **6. Fase de Planificación**

### **6.1 Contexto**

#### **6.1.1 Comprensión de la organización y su contexto.**

En el IDEA se tiene identificado el presente contexto; durante el presente año se adecuará el análisis de Contexto de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONEXTO DE LA ORGANIZACIÓN de la norma ISO 27001, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 12</b>

### **6.1.2 Alcance**

El Modelo de Seguridad y privacidad de la Información MSPI aplica a la estructura del Modelo de Operaciones por Procesos del IDEA, a todos los usuarios internos y externos (Gerentes, Directivos, Servidores públicos funcionarios vinculados de planta, permanente y provisional, contratistas, consultores, practicantes, proveedores y entes de control) y todas las partes interesadas que presten sus servicios o tengan algún tipo de relación con la información del Instituto para el desarrollo de Antioquia – IDEA-, por consiguiente, aplicará a la estructura del Modelo de Operaciones por Procesos del Instituto.

## **6.2 Liderazgo**

### **6.2.1 Liderazgo y Compromiso**


Se realiza la modificación de la estructura organizacional, y se definió la Dirección de Ciberseguridad y Seguridad de la Información, se establece que desde la Dirección de Ciberseguridad y Seguridad de la Información se debe asegurar la implementación del Sistema de Seguridad de la Información y Ciberseguridad

### **6.2.2 Política de Seguridad de la Información y Ciberseguridad**

La Junta Directiva del Instituto aprueba la Política de Seguridad de la Información y Ciberseguridad como muestra de su compromiso y apoyo en el diseño e implementación del Modelo de Seguridad y Privacidad de la Información en el IDEA para garantizar la gestión de estos aspectos en la entidad.

Con relación a los documentos de operación del sistema de seguridad de la información y en cumplimiento a lo establecido en la norma ISO 27001, la entidad cuenta con la siguiente documentación:

- Declaración de aplicabilidad
- Guía para la Gestión de Activos de Información
- Sistema de Administración de Riesgos de Seguridad de la Información y Ciberseguridad
- Procedimiento Plan de Continuidad del Negocio

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 13</b>

- Procedimiento Gestión de Incidentes de seguridad de la información y Ciberseguridad

Entre otros.

En el año 2025 se elaborará la documentación que complemente los documentos para la operación del Sistema de Seguridad de la Información.

### **6.2.3 Roles y Responsabilidades**

En el año 2023 se asignan las funciones en materia de protección de la información y se establece el comité de Ciberseguridad y de la Información.


En cuanto a la matriz de roles y responsabilidades de las áreas del IDEA frente al Sistema de Gestión de Seguridad de la Información y Ciberseguridad será elaborada durante el presente período

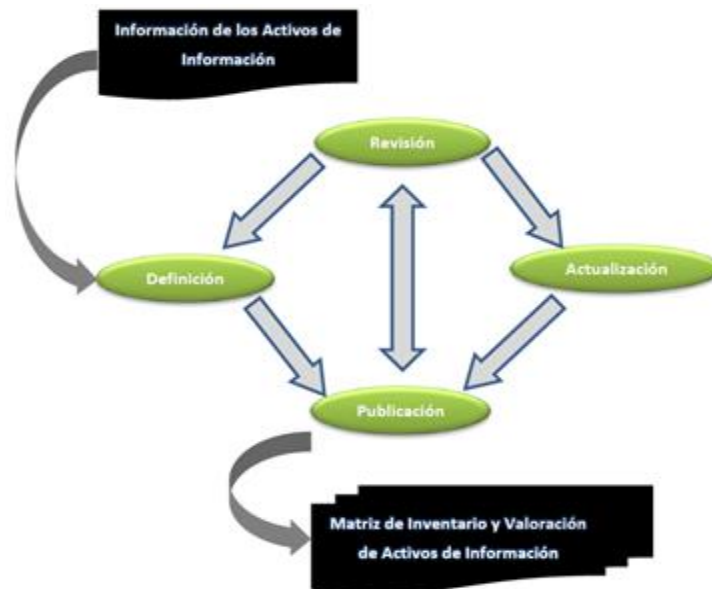
## **6.3 Planificación**

### **6.3.1 Identificación de activos de información e infraestructura crítica**

La identificación de activos de información en el IDEA se realiza tomando como lineamientos lo establecido en la Guía para la Gestión de Activos de Información.

La identificación, creación, actualización, modificación, supresión o inactivación de un activo de información se realiza en el aplicativo dispuesta para tal fin, la actividad de identificación y actualización se realiza anualmente.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>		
	<b>Plan de Seguridad y Privacidad de la Información</b>		
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>
			<b>Pagina 14</b>



Grafica 2 Actividades para elaborar Inventario de Activos de Información "Tomado de: Guía para Gestión de Activos de Información "

### 6.3.2 Valoración de los riesgos de seguridad de la información

El IDEA cuenta con un Marco para la Gestión de Riesgos y un sistema que facilita la integración de riesgos en todas las actividades y define los parámetros para su identificación, análisis, valoración, tratamiento, monitoreo y análisis de riesgos residual; la metodología se describe en Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad – SARSIC.


La identificación, creación, actualización, modificación, tratamiento, monitoreo y evaluación del riesgo residual de un riesgo de seguridad de la información y ciberseguridad se realiza en el aplicativo dispuesto para tal fin.

Las actividades para desarrollarse para el presente Ítem se detallan en la Tabla Plan de Seguridad y Privacidad de la Información.

### 6.3.3 Gestión de Incidentes de Seguridad

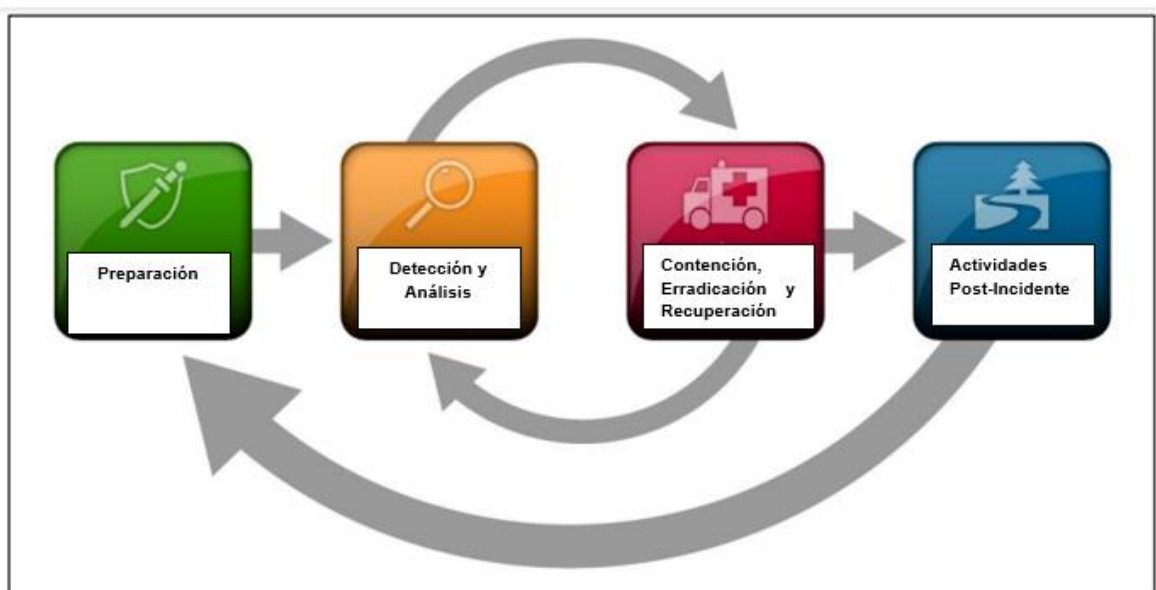
La gestión de Incidentes se implementa en el IDEA bajo el Procedimiento de Gestión de Incidentes de Seguridad de la Información y Ciberseguridad, los insumos para identificar los incidentes son:

- Sistemas de Prevención de Intrusiones (IPS)

	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD		
	Plan de Seguridad y Privacidad de la Información		
	Código:	Versión :03	Fecha de emisión: 2025
			Pagina 15


- Gestión de Eventos de Seguridad de la Información (SIEM)
- Antivirus, antispam y Protección de Amenazas Avanzadas (ATP)
- Registros del sistema operativo, servicios y aplicaciones
- Registros de dispositivos de red
- Información sobre nuevas vulnerabilidades y exploits
- Usuarios Internos
- Usuarios Externos

Las fases principales del proceso de respuesta a incidentes son la preparación, detección y análisis, contención, erradicación y recuperación, y actividad posterior al incidente, en detalle.



*Ilustración 3. Ciclo de vida para la respuesta a Incidentes de seguridad de la información, NIST.*

Para una atención adecuada a los incidentes (análisis, contención y erradicación) se determinará el nivel de prioridad de este, y de esta manera se atenderá adecuadamente.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>		
	<b>Plan de Seguridad y Privacidad de la Información</b>		
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>
			<b>Pagina 16</b>

## **6.4 Soporte**

### **6.4.1 Recursos**

El Instituto para el Desarrollo de Antioquia ha designado y proporcionado recursos económicos necesarios para adoptar el Modelo de Seguridad y Privacidad de la Información el cual Monitoreo de Amenazas con el SOC, Identificación de Activos, Valoración y tratamiento de Riesgos, Manejo de Incidentes de Seguridad y Ciberseguridad, Elaboración de pruebas de vulnerabilidades, concientización en Seguridad de la Información, Protección de datos personales, cómo parte del compromiso y liderazgo de la alta dirección de acuerdo, donde se estipulan los recursos para la Dirección de Ciberseguridad y Seguridad de la Información.

### **6.4.2 Competencia, toma de conciencia y comunicación**

Con la finalidad de sensibilizar a los funcionarios, contratistas y demás partes interesadas del IDEA respecto al Sistema de Gestión de Seguridad y Privacidad de la Información, el Instituto cuenta con:


- Plan anual de sensibilización, mediante el cual se diseñan y construyen piezas de comunicación, sobre temas de seguridad de la información y ciberseguridad, las cuales, son divulgadas periódicamente a través de los diferentes canales oficiales de comunicación del Instituto.
- Charlas de Sensibilización en temas de seguridad de la información y ciberseguridad.
- Campañas de comunicación en los medios oficiales de la Institución

Las demás actividades enfocadas a la toma de conciencia por parte de los funcionarios, contratistas y proveedores se detallan en el cuadro Plan de Seguridad y Privacidad de la Información.

## **7. Fase de Operación**

En esta fase se llevará a cabo la implementación del Sistema de Gestión. Los responsables deberán ejecutar, planear y desarrollar las actividades que permitan fortalecer el Sistema de Gestión de Ciberseguridad y Seguridad de la Información institucional. Como parte de la planeación, se deberá tener en cuenta los recursos



	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Página 17</b>

necesarios (humanos, tecnológicos, financieros), e identificar y gestionar los riesgos que dichas actividades pueden con llevar.

### 7.1 Planificación e implementación

Para la implementación de la fase de planificación del Sistema de Seguridad de la Información, se tuvo en cuenta los aspectos más relevantes que según el análisis del instrumento evaluación ISO 27001:2022 y Ciberseguridad nos indicó los temas a fortalecer y los necesarios a mantener con la finalidad de establecer Sistema de Gestión de Seguridad de la Información de la Institución. Las siguientes son actividades que se desarrollan dentro de un proceso de mejora continua; actividades que serán evaluadas en su cumplimiento y discutido en el comité de Ciberseguridad y Seguridad de la Información.

#### *Plan de Seguridad y Privacidad de la Información*

Requisito	Sub requisito/Control ISO 27001:2022	Implementación	Actividad	2025	
				Fecha Inicio	Fecha Final
4. Contexto de la Organización	4.2. Comprender las necesidades y expectativas de las partes interesadas	Contexto de la Organización	Implementación de la Herramienta	20/01/2025	30/03/2025
	4.3. Determinación del alcance del Sistema de Gestión de Seguridad de la Información	Declaración de aplicabilidad	Declaración de Aplicabilidad	1/10/2025	30/11/2025
	4.4. Sistema de Gestión de Seguridad de la Información y 7.5.1. Información documentada	SGSI	Nueva Documentación del SGSI establecer Formatos, nuevas políticas, procedimiento entre otros.	20/01/2025	30/11/2025
5. Liderazgo	5.2. Política	Política	Revisar la política de Seguridad de la Información para identificar temas que requieran actualización	30/01/2025	30/11/2025
			Identificar necesidades teniendo en cuenta el cambio del entorno y normatividad	30/01/2025	30/11/2025
			Actualización del Manual de Políticas de Seguridad de la Información	30/01/2025	30/11/2025



# SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

## Plan de Seguridad y Privacidad de la Información


**Código:**

**Versión :03**


**Fecha de emisión:**  
**2025**

**Pagina 18**

Activos de Información	5.9. Inventario de Información y otros activos asociados	Activos	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique	1/02/2025	30/06/2025
			Validar activos de información con el inventario realizado en el año anterior con cada uno de los procesos	1/02/2025	30/06/2025
			Identificar nuevos activos de información	1/02/2025	30/06/2025
	5.10. Uso aceptable de la información y otros activos asociados		Acta de aceptación de los activos de información para cada uno de los procesos	1/02/2025	30/06/2025
			Consolidar el inventario de Activos de Información	1/02/2025	30/06/2025
			Registrar los Activos de Información	1/02/2025	30/04/2025
			6. Planificación y 8. Operación	6.1. Acciones para abordar riesgos y oportunidades y 8.3 Tratamiento de riesgos de Seguridad de la Información	Riesgos
Validar riesgos de Seguridad de la Información, Ciberseguridad y Protección de datos personales con los riesgos del año anterior	1/03/2025	15/12/2025			
Identificar nuevos Riesgos tomando como insumo el inventario de Activos de Información y los que se presenten durante el periodo por identificación	1/03/2025	15/12/2025			
6.1.2. y 8.2. Evaluación de los riesgos de seguridad de la información					
	Evaluar los riesgos de Seguridad de la información de acuerdo con el SARSIC	1/03/2025		15/12/2025	
6.1.3. y 8.3. Tratamiento de Riesgos de Seguridad de la Información	Formular un plan de tratamiento de los riesgos de Seguridad de la Información	1/03/2025		15/12/2025	
	Acta de Aceptación de los Riesgos	1/03/2025		15/12/2025	
	Registro de los Riesgos en el aplicativo	1/03/2025		15/12/2025	
	Seguimiento al plan de tratamiento de riesgos	1/03/2025		15/12/2025	
	Evaluación del Riesgo Residual	1/03/2025		15/12/2025	
	Acta de aceptación riesgos residuales	1/03/2025		15/12/2025	
7. Soporte	7.2. Competencia 6.3. Concientización, educación y capacitación en seguridad de la información	Cambio y Cultura	Establece y ejecutar Plan de Cambio y Cultura	1/02/2025	15/12/2025
			o Socializar métodos de reporte de incidentes de Seguridad de la Información	1/02/2025	15/12/2025
	7.3. Conciencia		o Evaluaciones (ajustar con la circular de Superfinanciera)	1/02/2025	15/12/2025
			o Pruebas de Ingeniería Social	1/02/2025	15/12/2025
			o Encuestas de percepción de la Seguridad de la Información en el IDEA	1/02/2025	15/12/2025

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 19</b>

<b>Incidentes de Seguridad</b>	<b>5.26. Respuesta a incidentes de seguridad de la información</b>	<b>Incidentes</b>	Documentación y Registro de los incidentes presentados y cuadro de seguimiento	1/01/2025	31/12/2025
<b>8. Controles Tecnológicos</b>	<b>8.8. Gestión de Vulnerabilidades Técnicas</b>	<b>Vulnerabilidades</b>	Documentar la Guía de Gestión de Vulnerabilidades	1/01/2025	31/12/2025
			Realizar un inventario de los sistemas del IDEA	1/02/2025	31/12/2025
			Realizar pruebas de vulnerabilidades sobre los sistemas críticos	1/02/2025	31/12/2025
			Presentar a la Dirección de Tecnología los resultados obtenidos en las pruebas de vulnerabilidades	28/02/2025	31/12/2025
			Hacer seguimiento al plan de acción establecido por la Dirección de Tecnología	28/02/2025	31/12/2025
<b>Ciber</b>	<b>Zero Trust</b>	<b>Zero Trust</b>	Identificar todos los dispositivos, usuarios y aplicaciones para implementar el modelo	1/02/2025	31/12/2025
	<b>8.2. Derechos de acceso privilegiado</b>		Verificar que los equipos tengan el mínimo de acceso	1/02/2025	31/12/2025
	<b>8.5. Autenticación Segura</b>		Verificar que se haya implementado el MFA en estos equipos	1/02/2025	31/12/2025
	<b>8.7. Protección contra malware</b>		Analizar vulnerabilidades en los dispositivos	1/02/2025	31/12/2025
	<b>8.16. Actividades de Seguimiento</b>		Analizar los informes remitidos por el SOC, y CSIRT	1/02/2025	31/12/2025
<b>10 Mejora</b>	<b>10.1. Mejora continua 5.30. Preparación de las TIC para la continuidad del negocio</b>	<b>Plan de Continuidad del Negocio</b>	Participar en las pruebas que realice la Gerencia de Riesgos	1/09/2025	31/12/2025
			Validar requisitos de seguridad de la información en cada prueba	1/09/2025	31/12/2025
			Identificar riesgos de seguridad de la información en cada prueba	1/09/2025	31/12/2025
			Documentar lecciones aprendidas	1/09/2025	31/12/2025
<b>5. Organizacionales</b>	<b>5.31. Requisitos legales, estatutarios, reglamentarios y contractuales</b>	<b>Requisitos Legales</b>	Listar los requerimientos de la legislación, regulación, normas, directivas a las cuales se les debe dar cumplimiento	1/10/2025	30/11/2025
			Diseñar el catálogo normativo donde se documente, actualicen todos los requerimientos	1/10/2025	30/11/2025
			Validar el cumplimiento de los requisitos legales	1/10/2025	30/11/2025
			Cargar en el aplicativo de gestión el catálogo y el cumplimiento	1/10/2025	30/11/2025


	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 20</b>

9. Evaluación de desempeño	9.1. Seguimiento, medición, análisis y evaluación	Indicadores	Establecer los indicadores del Proceso y del Sistema de Gestión de Seguridad de la Información	1/02/2025	28/02/2025
			Incluir los indicadores en al aplicativo de gestión	1/03/2025	30/03/2025
			Establecer métodos de evaluación	1/03/2025	30/03/2025
			Realizar seguimiento al cumplimiento de los indicadores	1/01/2025	31/12/2025
			Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad de la Información.	1/01/2025	30/01/2025
			Desarrollar la herramienta de autodiagnóstico general de Política de Gobierno Digital suministrada por MIPG	1/01/2025	30/01/2025
			Definir las estrategias basado en el resultado del autodiagnóstico	1/01/2025	30/01/2025
			Medir la efectividad de las estrategias desarrollando nuevamente la herramienta de autodiagnóstico	1/12/2025	30/12/2025
Gestión de datos personales	Protección de datos personales	Protección de Datos Personales	Capacitación de los funcionarios en ley 1581 de 2012.	1/02/2025	15/12/2025
			Realizar un inventario de las Base de datos personales que el IDEA maneja	1/02/2025	15/12/2025
			Actualizar las políticas sobre la recolección, uso y almacenamiento de datos personales.	1/02/2025	15/12/2025
			Establecer procedimientos para la gestión de solicitudes de acceso a datos, modificación y eliminación de información.	1/02/2025	15/12/2025

## 8. Fase de Evaluación de Desempeño

Una vez implementadas y desarrolladas las actividades del Plan de Seguridad y Privacidad de la Información y con la finalidad de realizar seguimientos, mediciones, análisis y evaluaciones al Sistema de Gestión de la Seguridad de la Información y al Modelo de Seguridad y Privacidad, a la Gestión de Riesgos, la efectividad del plan de sensibilización y al programa de Protección de Datos Personales se procede a evaluar para medir la efectividad de las acciones tomadas a través de indicadores.


El proceso de seguimiento y monitoreo del Modelo de Seguridad y Privacidad de la Información se hará al finalizar el periodo tomando como insumos las actividades ejecutadas en el Plan de Seguridad y Privacidad de la Información.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>		
	<b>Plan de Seguridad y Privacidad de la Información</b>		
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>
			<b>Pagina 21</b>

### 8.1 Seguimiento, medición, análisis y evaluación

El Sistema de Gestión de Seguridad de la Información tiene definidos los siguientes indicadores dentro del proceso de Ciberseguridad y Seguridad de la Información, con la finalidad de medir el cumplimiento de la ejecución de los controles relevantes del sistema:

<b>Nombre</b>	<b>Índice</b>	<b>Frecuencia de Medición</b>
Efectividad del plan de sensibilización	Número de empleados que suministraron la información/ Número de empleados elegidos para las pruebas de ingeniería social.	Trimestral
Gestión de las vulnerabilidades de Seguridad de la Información y Ciberseguridad	Número de vulnerabilidades (críticas y altas) / Número de vulnerabilidades (críticas y altas) encontradas en las pruebas de seguridad	Trimestral
Gestión de Incidentes de seguridad en la información y ciberseguridad	Número de incidentes de seguridad de la información y ciberseguridad (críticos y altos) gestionados/ Número de incidentes de seguridad de la información y ciberseguridad (críticos y altos) reportados	Trimestral
Madurez del modelo de seguridad de la información y ciberseguridad	Evaluación de efectividad de controles - ISO 27001:2022 Anexo A+ Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA)+ Nivel de madurez del Modelo de Seguridad de la Información y ciberseguridad+ Calificación frente a mejores prácticas NIST	Anual
Indicador de mitigación de riesgos de categoría mayor y extremo	Riesgos de categoría menor y extremo identificados/Riesgos de categoría mayor y extremo con plan de mitigación	Semestral

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 22</b>

## **8.2 Auditoría Interna**

El Instituto debe generar un documento donde se especifique el plan de auditorías para el Sistema de Gestión de Seguridad de la Información, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

## **8.3 Revisión por la Dirección**


Los temas de Seguridad de la Información y Ciberseguridad, medición de indicadores del sistema de gestión de seguridad, cumplimiento del plan de tratamiento de los riesgos, identificación de activos de información, seguimiento a las actividades del Plan de Seguridad y Privacidad de la Información, cumplimiento de la protección de datos personales la Política y demás temas relacionados con Seguridad de la Información y Ciberseguridad, son tratados y aprobados en el Comité de Ciberseguridad y Seguridad de la Información. De acuerdo con lo anterior el director de Ciberseguridad y Seguridad de la Información presenta los temas más relevantes.

## **9. Fase de Mejoramiento Continuo**

En esta fase el Instituto deberá consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad de la información y ciberseguridad, tomando las acciones oportunas para mitigar las debilidades identificadas.

### **9.1 Mejora**

Conforme a los resultados obtenidos en 9.1 Seguimiento, medición, análisis y evaluación, se debe tomar las acciones correspondientes para cumplir con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información y protección de Datos Personales y llegar al nivel de cumplimiento esperado según la escala de valoración de la herramienta Instrumento de Evaluación ISO 27001 y Ciberseguridad, se debe realizar seguimiento a las acciones para el cierre de brechas propuestas.

	<b>SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD</b>			
	<b>Plan de Seguridad y Privacidad de la Información</b>			
	<b>Código:</b>	<b>Versión :03</b>	<b>Fecha de emisión: 2025</b>	<b>Pagina 23</b>

## 10. Control de Cambios

Versión	Fecha	Descripción de Cambios
3	Enero de 2025	Versión 3, que reemplaza lo definido en la versión 2. Se actualizó el documento alineando los capítulos al MSPI versión 4 emitido el 22/02/2021 por el Ministerio de Tecnologías de la Información y las Comunicaciones.

<b>Elaboró:</b>	Yaritza Shirley Montoya Bolívar	Contratista	Dirección de Ciberseguridad y seguridad de la Información.
<b>Revisó:</b>	William René Alvarado Ordoñez	Director	Dirección de Ciberseguridad y Seguridad de la Información.
<b>Aprobó:</b>	William René Alvarado Ordoñez	Director	Dirección de Ciberseguridad y Seguridad de la Información.