


| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 1 |

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Modelo de Seguridad y Privacidad de la Información

IDEA

2026




| | | | | |
|---|---|-------------|---------------------------|----------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 2 |

Tabla de contenido

| | |
|---|-----------|
| INTRODUCCIÓN..... | 4 |
| 1. OBJETIVO..... | 4 |
| 2. ALCANCE..... | 5 |
| 3. DEFINICIONES | 5 |
| 4. DOCUMENTOS DE REFERENCIA | 7 |
| 5. CICLO DE OPERACIÓN..... | 11 |
| 6. Fase de Diagnóstico | 12 |
| 6.1 Instrumento de Evaluación Modelo de Seguridad y Privacidad de la Información 2026 | |
| 12 | |
| 6.1.1 Levantamiento de información | 12 |
| 6.1.2 Desarrollo | 13 |
| 6.1.3 Análisis de la Información..... | 13 |
| 6.1.4 Resultados | 13 |
| 7. Fase de Planificación..... | 17 |
| 7.1 Contexto | 18 |
| 7.1.1 Comprensión de la organización y su contexto..... | 18 |
| 7.1.2 Alcance | 18 |
| 7.2 Liderazgo..... | 19 |
| 7.2.1 Liderazgo y Compromiso | 19 |
| 7.2.2 Política de Seguridad de la Información y Ciberseguridad | 19 |
| 7.2.3 Roles y Responsabilidades | 19 |
| 7.3 Planificación | 20 |
| 7.3.1 Identificación de activos de información e infraestructura critica | 20 |
| 7.3.2 Valoración de los riesgos de seguridad de la información | 20 |
| 7.3.3 Gestión de Incidentes de Seguridad | 21 |
| 7.4 Soporte | 22 |
| 7.4.1 Recursos | 22 |

| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 3 |

| | | |
|------------|--|-----------|
| 7.4.2 | Competencia, toma de conciencia y comunicación | 23 |
| 8. | <i>Fase de Operación.....</i> | 23 |
| 8.1 | Implementación | 23 |
| 9. | <i>Fase de Evaluación de Desempeño</i> | 27 |
| 9.1 | Seguimiento, medición, análisis y evaluación | 28 |
| 9.2 | Auditoría Interna | 28 |
| 9.3 | Revisión por la Dirección..... | 29 |
| 10. | <i>Fase de Mejoramiento Continuo</i> | 29 |
| 10.1 | Mejora Continua | 29 |
| 10.2 | Acciones Correctivas y no conformidades..... | 29 |
| 11. | <i>Control de Cambios</i> | 30 |

| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 4 |

INTRODUCCIÓN

En cumplimiento de lo establecido en el artículo 2.2.22.3.14 del Decreto Único Reglamentario del Sector de Función Pública (Decreto 1083 de 2015, adicionado por el Decreto 612 de 2018), que exige la integración de los planes institucionales y estratégicos al Plan de Acción y su publicación anual, se actualiza el Plan de Seguridad y Privacidad de la Información del Instituto para el Desarrollo de Antioquia – IDEA, incorporándolo plenamente al Plan de Acción institucional.

Para llevar a cabo la implementación del MSPI se debe contar con el Plan de Seguridad y Privacidad de la Información.


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.

El presente documento brinda el marco de referencia, 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.

1. OBJETIVO

Definir el Plan de Seguridad y Privacidad de la Información MSPI en el IDEA y establecer las actividades a desarrollarse durante el año 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

| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 5 |


(Planear, Hacer, Verificar y Actuar); acorde con la norma NTC ISO/IEC 27001:2022, la normativa vigente y los criterios de continuidad de la operación de los servicios que permitan mantener la seguridad y privacidad de la información en los procesos del IDEA.

2. ALCANCE


El presente documento aplica a todo el modelo de operación por procesos del Instituto para el Desarrollo de Antioquia – IDEA, dando cumplimiento a lo establecido en el Decreto 1083 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, al Capítulo 1 del Título 9 del Decreto 1078 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, así como el Modelo de Seguridad y Privacidad de la Información de la Resolución 500 de 2021 y la actualización del Anexo 1 en la resolución 02277 de 2026, alineado con la NTC/IEC ISO 27001.

3. 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, 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).

| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 6 |


- 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)
- 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).

| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 7 |


- 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).
- 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.

4. 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:


| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 8 |

- Constitución Política de Colombia. Artículos 15, 20, 23, 74, referente al derecho al habeas data, el derecho a la intimidad, el derecho a la información, derecho de petición y derecho de acceso a la información pública
- Constitución Política de Colombia. Artículos: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
- CONPES 3995 de 2020. Confianza y Seguridad Digital
- CONPES 3854 de 2017. Política Nacional de Seguridad digital.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3975 del 2019 política nacional para la transformación digital e inteligencia artificial
- CONPES 4069 de 2022. Política Nacional de Ciencia, tecnología e innovación 2022 – 2031.
- CONPES 4144 de 2026. Política Nacional de Inteligencia Artificial
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 338 de 2022, el cual fortaleció la gobernanza en seguridad digital y estableció lineamientos para la identificación de Infraestructuras Críticas Cibernéticas (ICC) y Servicios Esenciales (SE)
- 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 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- 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


| | | | | |
|---|--|--------------------|-----------------------------------|-----------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 9 |

del orden nacional 21 del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico

- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- 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.
- 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”.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- 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 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.
- 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 2364 de 2012, por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 10 |

- Directiva 26 de 2020, diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014
- Ley 1221 de 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 1581 de 2012. Por la cual 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 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 1755 de 2015, por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- 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
- Ley 2052 de 2020, por medio de la cual se expide el Código General Disciplinario, se deroga la Ley 734 de 2002 y se dictan otras disposiciones
- Resolución 746 de 2022, "por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
- Resolución 1838 de 2022, "por la cual se reglamentan las modalidades de teletrabajo, se establecen las condiciones de trabajo en casa y se definen los lineamientos de desconexión laboral en el MINTIC, y se deroga la resolución 1151 del 16 de mayo de 2019"


| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 11 |

- Resolución 02277 de 2026, el Ministerio TIC actualiza el Modelo de Seguridad y Privacidad de la Información
- Resolución 20231045 “Por medio del cual se actualiza la versión No. 1 de la Política de Protección de Datos Personales del Instituto para el Desarrollo de Antioquia - IDEA”
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Norma ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.

5. 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 5, 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.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 12 |

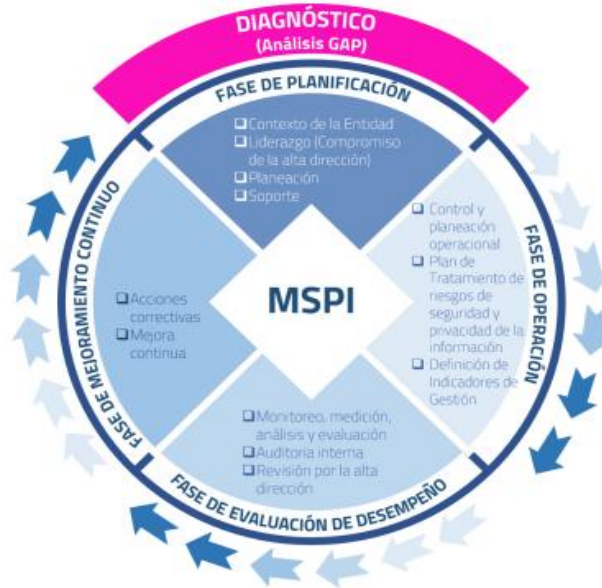


Figura 1 - Ciclo Modelo de Seguridad y Privacidad de la Información (Tomado MSPI - Min Tic V4)

6. 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.

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 Modelo de Seguridad y Privacidad de la Información 2026.


6.1 Instrumento de Evaluación Modelo de Seguridad y Privacidad de la Información 2026

Este Instrumento, es la herramienta de autodiagnóstico del MSPI 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:

6.1.1 Levantamiento de información

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

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 13 |

6.1.2 Desarrollo

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


6.1.3 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.
- Avance PHVA: se determina el nivel de cumplimiento del ciclo PHVA del Modelo, incluyendo los siguientes componentes:
 - Planificación
 - Implementación
 - Evaluación de desempeño
 - Mejora Continua
- Ciberseguridad: Se determina como se encuentra el Instituto frente a las mejores prácticas en ciberseguridad.

6.1.4 Resultados

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

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


| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 14 |

de controles del Documento Maestro de los Lineamientos del Modelo de Seguridad de Privacidad de la información.

- Escala de Evaluación

Muestra la posible calificación que se puede dar a cada criterio:

| Tabla de Escala de Valoración de Controles ISO 27001:2022 ANEXO A | | |
|--|---------------------|--|
| Descripción | Calificación | Criterio |
| No Aplica | N/A | No aplica. |
| Inexistente | 0 | Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles. |
| Inicial | 20 | 1) Hay una evidencia que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican. |
| Repetible | 40 | Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores. |
| Efectivo | 60 | Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada. |
| Gestionado | 80 | Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente. |
| Optimizado | 100 | Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas , basándose en los resultados de una mejora continua. |

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 15 |

En la Evaluación de Efectividad de controles se obtuvieron los siguientes resultados:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

| No. | Evaluación de Efectividad de controles | | | Nivel de Madurez |
|---|--|---------------------|-----------------------|-------------------|
| | DOMINIO | Calificación Actual | Calificación Objetivo | |
| A.5 | CONTROLES ORGANIZACIONALES | 84 | 100 | OPTIMIZADO |
| A.6 | CONTROLES DE PERSONAS | 93 | 100 | OPTIMIZADO |
| A.7 | CONTROLES FÍSICOS | 90 | 100 | OPTIMIZADO |
| A.8 | CONTROLES TECNOLÓGICOS | 66 | 100 | GESTIONADO |
| PROMEDIO EVALUACIÓN DE CONTROLES | | 83 | 100 | OPTIMIZADO |

BRECHA ANEXO A ISO 27001:2022



AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA)



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Plan de Seguridad y Privacidad de la Información

Código:P-SSI-001

Versión :04

**Fecha de emisión:
2026**


Pagina 16

MODELO FRAMEWORK CIBERSEGURIDAD NIST

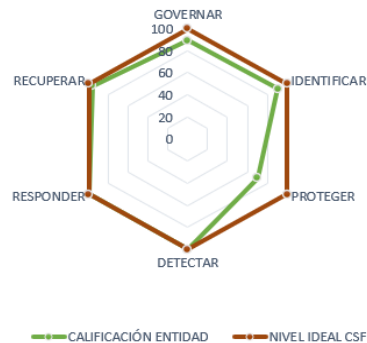
| Etiquetas de fila | CALIFICACIÓN ENTIDAD | NIVEL IDEAL CSF |
|--------------------------|-----------------------------|------------------------|
| GOVERNAR | 89 | 100 |
| IDENTIFICAR | 91 | 100 |
| PROTEGER | 70 | 100 |
| DETECTAR | 100 | 100 |
| RESPONDER | 100 | 100 |
| RECUPERAR | 96 | 100 |

| AÑO | COMPONENTE (PHVA) | CLAUSULAS | % de Avance Actual | % Avance Esperado |
|--------------|--------------------------------|-----------------------------|---------------------------|--------------------------|
| 2025 | Planificación | Contexto de la organización | 14% | 14% |
| | | Liderazgo | 14% | 14% |
| | | Planificación | 14% | 14% |
| | | Soporte | 13% | 14% |
| | Implementación | Operación | 16% | 16% |
| | Evaluación de Desempeño | Evaluación del desempeño | 12% | 14% |
| | Mejora Continua | Mejora | 11% | 14% |
| TOTAL | | | 95% | 100% |

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 17 |

BRECHA NIST



El resultado obtenido para la evaluación del estado para la vigencia 2025, refleja el estado actual de los controles implementados en el IDEA.

Los resultados permiten identificar el nivel de madurez alcanzado en materia de seguridad de la información y constituyen una base para la mejora continua del sistema de gestión


De acuerdo con los resultados, se inicia un plan de mejoramiento para mejorar la calificación.

7. Fase de Planificación

Durante la fase de planeación del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con los resultados de la fase anterior, se definen las tareas, acciones y resultados esperados en materia de seguridad y privacidad de la información, el Plan de Seguridad y Privacidad de la Información el cual debe:

- **Estar alineada con los objetivos institucionales** y los lineamientos estratégicos.
- **Incluir medidas específicas de protección**, fundamentadas en una metodología de gestión de riesgos que permita priorizar acciones y optimizar la asignación de recursos.
- Considerar los recursos necesarios para su ejecución, entre ellos:

Recursos Humanos: equipo de seguridad de la información, líderes de áreas estratégicas y comité de seguridad.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 18 |

Recursos Tecnológicos: herramientas para análisis de riesgos, plataformas de gestión documental y sistemas de monitoreo.

Recursos Financieros: presupuesto para consultoría, adquisición de tecnología y capacitación.

La correcta ejecución de esta fase establece una base sólida para la implementación progresiva de controles, la mitigación de riesgos y el fortalecimiento del entorno de seguridad digital del IDEA. Su propósito es mejorar las condiciones de protección de la información en todos los procesos y áreas institucionales, garantizando la coherencia con los objetivos estratégicos y el cumplimiento de la normatividad vigente.


7.1 Contexto

7.1.1 Comprensión de la organización y su contexto.

Durante el presente año se actualizará el análisis de Contexto de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONTEXTO 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.

7.1.2 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.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 19 |

7.2 Liderazgo

7.2.1 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

7.2.2 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
- Procedimiento Gestión de Incidentes de seguridad de la información y Ciberseguridad

Entre otros.

En el año 2026 se elaborará la documentación que complemente los documentos para la operación del Sistema de Seguridad de la Información.

7.2.3 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.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 20 |

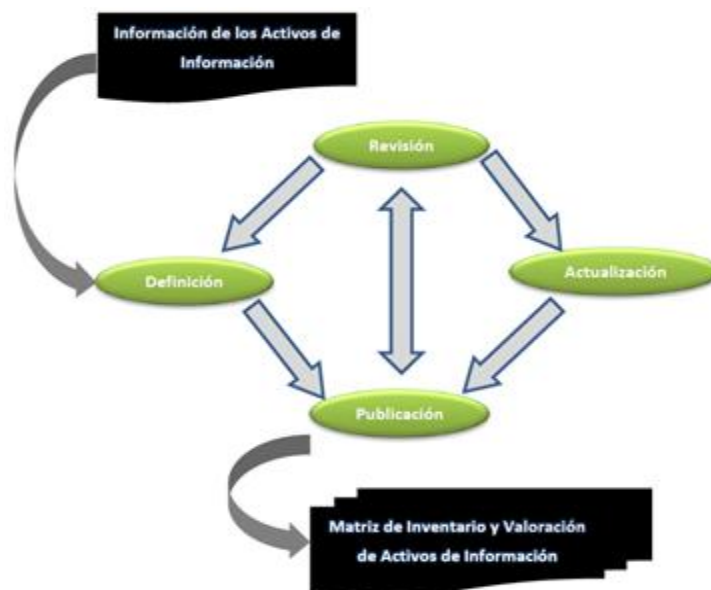
En cuanto a la matriz de roles y responsabilidades de las áreas del IDEA frente al Sistema de Gestión de Seguridad de la Información y Ciberseguridad será actualizada durante el presente período

7.3 Planificación

7.3.1 Identificación de activos de información e infraestructura critica

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.



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

7.3.2 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

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 21 |

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.

7.3.3 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:

- 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.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 22 |

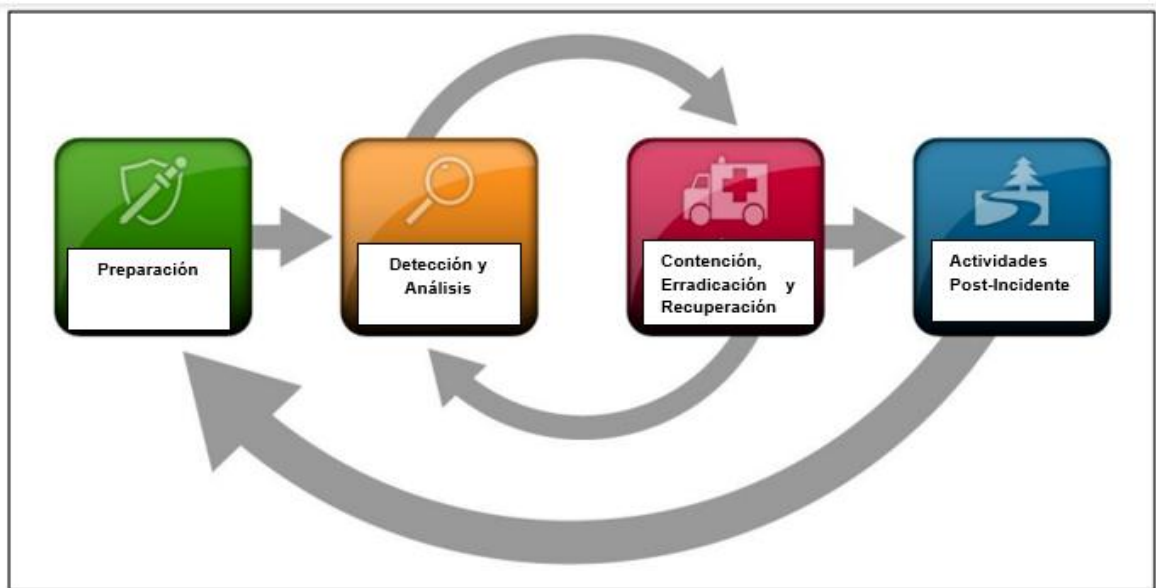



Ilustración 3. Ciclo de vida para la respuesta a Incidentes de seguridad de la información, NIST.

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.

7.4 Soporte

7.4.1 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.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 23 |

7.4.2 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
 - Pruebas de Ingeniería Social


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.

8. 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.

8.1 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 de autoevaluación del Modelo de Seguridad y Privacidad de la Información 2026 nos indicó los temas a fortalecer y los necesarios a mantener con la finalidad de preservar el Sistema de Gestión de Seguridad de la Información del IDEA. 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.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 24 |


La implementación efectiva de esta fase fortalece la capacidad institucional para prevenir, detectar y responder a incidentes de seguridad, asegurando la continuidad operativa y el cumplimiento de los objetivos estratégicos.

Plan de Seguridad y Privacidad de la Información


| Requisito | Sub requisito/Control ISO 27001:2022/Ley 1581 | Implementación | Actividad | 2026 | |
|--------------------------------|---|------------------------------|---|--------------|-------------|
| | | | | Fecha Inicio | Fecha Final |
| 4. Contexto de la Organización | 4.2. Comprender las necesidades y expectativas de las partes interesadas | Contexto de la Organización | Actualización del Contexto | 20/01/2026 | 30/03/2026 |
| | 4.3. Determinación del alcance del Sistema de Gestión de Seguridad de la Información | Declaración de aplicabilidad | Actualización Declaración de Aplicabilidad | 1/10/2026 | 30/11/2026 |
| | 4.4. Sistema de Gestión de Seguridad de la Información y 7.5.1. Información documentada | SGSI | Actualización y nueva Documentación del SGSI establecer Formatos, nuevas políticas, procedimiento entre otros. | 20/01/2026 | 30/11/2026 |
| 5. Liderazgo | 5.2. Política | Política | Revisar la política de Seguridad de la Información para identificar temas que requieran actualización acorde al análisis de brechas 2025 | 30/01/2026 | 30/11/2026 |
| | | | Actualización del Manual de Políticas de Seguridad de la Información | 30/01/2026 | 30/11/2026 |
| 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, acorde al análisis de brechas 2025 | 1/02/2026 | 30/06/2026 |
| | | | Validar activos de información con el inventario realizado en el año 2025 con cada uno de los procesos | 1/02/2026 | 30/06/2026 |
| | | | Identificar nuevos activos de información | 1/02/2026 | 30/06/2026 |
| | 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 | 1/02/2026 | 30/06/2026 |
| | | | Consolidar el inventario de Activos de Información | 1/02/2026 | 30/06/2026 |
| | | | Registrar los Activos de Información en el aplicativo NOVASEC | 1/02/2026 | 30/06/2026 |

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 25 |

| | | | | | |
|---------------------------------|--|------------------|---|------------|------------|
| | | | Presentar al comité de Gestión los activos de información | | |
| | | | Publicar en G+ los activos de información | 1/02/2026 | 30/06/2026 |
| | | | Apoyar en la identificación, clasificación, valoración y rotulado de activos de los activos de información | 01/02/2026 | 01/12/2026 |
| | | | Trabajar conjuntamente con el CAD en el desarrollo de procedimientos, guías, instructivos y manuales del proceso de Centro de Administración Documental | 01/02/2026 | 01/12/2026 |
| 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 | Actualizar la metodología y lineamientos de la gestión de riesgos en caso de que aplique acorde al análisis de brechas 2025 | 1/03/2026 | 15/12/2026 |
| | | | Validar riesgos de Seguridad de la Información, Ciberseguridad y Protección de datos personales con los riesgos del año 2025 | 1/03/2026 | 15/12/2026 |
| | | | Identificar nuevos Riesgos tomando como insumo el inventario de Activos de Información y los que se presenten durante el periodo por identificación | 1/03/2026 | 15/12/2026 |
| | | | Presentar los riesgos de SI y CS al comité de gestión | 1/03/2026 | 15/12/2026 |
| | 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 | 1/03/2026 | 15/12/2026 |
| | 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 | 1/03/2026 | 15/12/2026 |
| | | | Acta de Aceptación de los Riesgos | 1/03/2026 | 15/12/2026 |
| | | | Registro de los Riesgos en el aplicativo NOVASEC | 1/03/2026 | 15/12/2026 |
| | | | Seguimiento al plan de tratamiento de riesgos | 1/03/2026 | 15/12/2026 |
| | | | Evaluación del Riesgo Residual | 1/03/2026 | 15/12/2026 |
| 7. Soporte | 7.2. Competencia 6.3. Concientización, educación y capacitación en seguridad de la información | Cambio y Cultura | Elaborar y ejecutar Plan de Cambio y Cultura | 1/02/2026 | 15/12/2026 |
| | | | Socializar métodos de reporte de incidentes de Seguridad de la Información | 1/02/2026 | 15/12/2026 |
| | | | Evaluaciones | 1/02/2026 | 15/12/2026 |
| | | | Pruebas de Ingeniería Social | 1/02/2026 | 15/12/2026 |
| | 7.3. Conciencia | | Encuestas de percepción de la Seguridad de la Información en el IDEA | 1/02/2026 | 15/12/2026 |

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 26 |

| | | | | | |
|-----------------------------------|---|--|--|------------|------------|
| Incidentes de Seguridad | 5.26. Respuesta a incidentes de seguridad de la información | Incidentes | Actualización del procedimiento de Gestión de Incidentes de Seguridad | 1/01/2026 | 31/12/2026 |
| | | | Socialziar el procedimiento de gestión de incidentes de Seguridad | 1/01/2026 | 31/12/2026 |
| 8. Controles Tecnológicos | 8.8. Gestión de Vulnerabilidades Técnicas | Vulnerabilidades | Actualizar la Guía de Gestión de Vulnerabilidades | 1/01/2026 | 31/12/2026 |
| | | | Apoyaren la ejecución de pruebas de vulnerabilidades sobre los sistemas | 1/02/2026 | 31/12/2026 |
| | | | Presentar a la Dirección de Tecnología los resultados obtenidos en las pruebas de vulnerabilidades | 28/02/2026 | 31/12/2026 |
| | | | Hacer seguimiento al plan de acción establecido por la Dirección de Tecnología de la remediación de vulnerabilidades | 28/02/2026 | 31/12/2026 |
| | 8.5. Autenticación Segura | | Verificar que todos los aplicativos cuenten con MFA | 1/02/2026 | 31/12/2026 |
| | 8.7. Protección contra malware | | Verificar la implementación del ZTNA | 1/02/2026 | 31/12/2026 |
| | 8.16. Actividades de Seguimiento | | Analizar los informes remitidos por el SOC, y CSIRT | 1/02/2026 | 31/12/2026 |
| 10 Mejora | 10.1. Mejora continua 5.30. Preparación de las TIC para la continuidad del negocio | Plan de Continuidad del Negocio | Participar en las pruebas que realice la Gerencia de Riesgos en continuidad del negocio | 1/09/2026 | 31/12/2026 |
| | | | Validar requisitos de seguridad de la información en cada prueba | 1/09/2026 | 31/12/2026 |
| | | | Identificar riesgos de seguridad de la información en cada prueba | 1/09/2026 | 31/12/2026 |
| | | | Documentar lecciones aprendidas en caso de que aplique | 1/09/2026 | 31/12/2026 |
| 5. Organizacionales | 5.31. Requisitos legales, estatutarios, reglamentarios y contractuales | Requisitos Legales | Actualizar el formato de requisitos legales | 1/10/2026 | 30/11/2026 |
| | | | Diseñar el catálogo normativo donde se documente, actualicen todos los requerimientos | 1/10/2026 | 30/11/2026 |
| | | | Validar el cumplimiento de los requisitos legales | 1/10/2026 | 30/11/2026 |
| 9. Evaluación de desempeño | 9.1. Seguimiento, medición, análisis y evaluación | Indicadores | Actualizar los indicadores del Sistema de Gestión de Seguridad de la Información | 1/02/2026 | 28/02/2026 |
| | | | Incluir los indicadores en al aplicativo de gestión | 1/03/2026 | 30/03/2026 |
| | | | Realizar seguimiento al cumplimiento de los indicadores | 1/01/2026 | 31/12/2026 |

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 27 |


| | | | | | |
|--|----------|--------------------------------|--|------------|------------|
| Privacidad y protección de la información de identificación personal (PII) | | | Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad de la Información. | 1/01/2026 | 30/01/2026 |
| | | | Implementar la herramienta de autodiagnóstico del MSPI suministrada por el Ministerio de las Tecnologías | 12/01/2026 | 30/12/2026 |
| | | | Definir las estrategias basado en el resultado del autodiagnóstico | 12/01/2026 | 30/12/2026 |
| | Ley 1581 | Protección de Datos Personales | Realizar un inventario de las Base de datos personales que el IDEA maneja | 1/02/2026 | 15/12/2026 |
| | | | Actualizar la política de protección de datos personales | 1/02/2026 | 15/12/2026 |
| | | | Actualizar las políticas sobre la recolección, uso y almacenamiento de datos personales. | 1/02/2026 | 15/12/2026 |
| | | | Establecer procedimientos para la gestión de solicitudes de acceso a datos, modificación y eliminación de información. | 1/02/2026 | 15/12/2026 |

9. 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 analiza y revisa la efectividad de las acciones implementadas para proteger la información, lo que implica la recopilación y el análisis de datos sobre auditorías internas y externas, y revisiones periódicas de cumplimiento.

El objetivo principal de esta fase es identificar las fortalezas y debilidades del sistema de gestión de seguridad de la información, así como evaluar la eficiencia y efectividad de los controles implementados. Los resultados obtenidos permiten a la Entidad tomar decisiones basadas en evidencia para ajustar y optimizar las políticas, procedimientos y mecanismos de seguridad y privacidad, garantizando una protección continua, integral y conforme a los requisitos normativos aplicables.

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.

| | | | |
|---|--|--------------------|-----------------------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | |
| | Plan de Seguridad y Privacidad de la Información | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 |
| Pagina 28 | | | |


9.1 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:

| Nombre | Índice | Frecuencia de Medición |
|--|---|-------------------------------|
| Efectividad del plan de sensibilización | Número de empleados que ganaron la evaluación (Calificación mínima 80) / Número de empleados evaluados | Anual |
| Madurez Operativa del Modelo de Zero Trust | Sumatoria del Porcentaje del cumplimiento de cada pilar | 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 gestión de riesgos de Ciberseguridad y Seguridad de la Información | Riesgos de categoría mayor y extremo identificados/Riesgos de categoría mayor y extremo con plan de acción | Semestral |

9.2 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

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Pagina 29 |

especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

9.3 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.

10. Fase de Mejoramiento Continuo


En esta fase el Instituto deberá consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar y ajustar acciones basadas en estos resultados, tomando las acciones oportunas para mitigar las debilidades identificadas.

10.1 Mejora Continua

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 de autodiagnóstico, se debe realizar seguimiento a las acciones para el cierre de brechas propuestas.

10.2 Acciones Correctivas y no conformidades

Ante una no conformidad, el IDEA debe corregirla, mitigar sus efectos y evaluar acciones para evitar su repetición.

| | | | | |
|---|--|--------------------|-----------------------------------|------------------|
|  | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD | | | |
| | Plan de Seguridad y Privacidad de la Información | | | |
| | Código:P-SSI-001 | Versión :04 | Fecha de emisión: 2026 | Página 30 |

11. Control de Cambios

| Versión | Fecha | Descripción de Cambios |
|---------|----------------|--|
| 3 | Enero de 2026 | 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. |
| 4 | Diciembre 2025 | Versión 4, que reemplaza lo definido en la versión 3. Se actualizó el documento alineando los capítulos al MSPI versión 5 emitido el 26/06/2025 por el Ministerio de Tecnologías de la Información y las Comunicaciones. |

| | | | |
|-----------------|---------------------------------|-------------|--|
| Elaboró: | Yaritza Shirley Montoya Bolívar | Contratista | Dirección de Ciberseguridad y seguridad de la Información. |
| Revisó: | William René Alvarado Ordoñez | Director | Dirección de Ciberseguridad y Seguridad de la Información. |
| Aprobó: | William René Alvarado Ordoñez | Director | Dirección de Ciberseguridad y Seguridad de la Información. |
| Elaboró: | Yaritza Shirley Montoya Bolívar | Contratista | Dirección de Ciberseguridad y seguridad de la Información. |
| Revisó: | Alexander Restrepo Zuluaga | Director | Dirección de Ciberseguridad y Seguridad de la Información. |
| Aprobó: | Alexander Restrepo Zuluaga | Director | Dirección de Ciberseguridad y Seguridad de la Información. |