PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE SALUD

Jefe de Oficina de Tecnología de la Información y Comunicaciones

Carlos Andrés López Fernández

Elaborado por:	Revisado por:	Aprobado por:
Sergio Andrés Ramos Pahuana Profesional Contratista OTIC Jesús David Diaz Quiceno Profesional Contratista OTIC	Carlos Andrés López Fernández Jefe OTIC	Carlos Andrés López Fernández Jefe OTIC Comité Institucional de Gestión y Desempeño Fecha Realización: 30/12/2025

Fecha de elaboración:

www.ins.gov.co

@INSColombia @insaludcolombia Instituto Nacional de Salud de Colombia

Avenida Calle 26 # 51 - 20 / Bogotá D.C. - Colombia PBX: (601) 220 77 00 / exts. 1101 - 1214 contactenos@ins.gov.co

1. INTRODUCCION

En Colombia se viene adelantando la implementación de la política pública de Gobierno Digital, establecido a través del decreto 1008 de 2018 en su artículo 2.2.9.1.1.3, definiendo la seguridad de la información como principio de dicha Política, de igual manera el Decreto 767 de 2022 en el artículo 2.2.9.1.2.1 define la estructura a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. Así mismo, el numeral 3.2 del mismo artículo define la Seguridad y Privacidad de la Información como habilitador que busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos, lo anterior articulado con el Modelo Integrado de Planeación y Gestión - MIPG, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo.

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI), es un documento que tiene como objetivo permitir a Instituto Nacional de Salud diseñar, planificar y ejecutar sus proyectos en materia de seguridad, alineándolo al MSPI del MinTIC en un corto, mediano y largo plazo, partiendo de un diagnóstico para identificar su estado actual y con ello ejecutar actividades que lo proyecten a un estado deseado en la protección de la información generada en el marco de la operación de sus procesos.

En el Instituto Nacional de Salud mediante la Resolución 1827 de 2022, en su artículo 18 expresa que: De acuerdo con las dimensiones y la política de gestión administrativa definidas en MIPG, se precisan los líderes de política e intervinientes como responsables de la adopción, mejoras y permanente seguimiento de las políticas en su calidad de voceros garantistas de su cumplimiento, que (…) la política de Gobierno digital y la política de seguridad digital (en donde se encuentra como habilitador el Modelo de Seguridad y Privacidad de la Información) serán responsables de la implementación la Oficina de Tecnologías de Información y las Comunicaciones – OTIC (…).

El manual interactivo de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que esta política tiene como objetivo impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de

los usuarios del ciberespacio. Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: Gobernanza e innovación pública digital, este último habilitado por cuatro elementos: Arquitectura, Cultura y apropiación, seguridad y privacidad de la información y, servicios ciudadanos digitales.

De igual manera el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (…) Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones (…).

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, cuyo propósito es servir como guía para la mejora de los estándares de seguridad en las entidades nacionales, la resolución 746 del 11 de marzo de 2022, por la cual se fortalece este modelo y se definen lineamientos adicionales a los establecidos en dicha resolución; y la resolución 02277 de 2025 que actualiza el Anexo 1 de la 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.

Así, en el marco de la evaluación de la Política de seguridad y Privacidad de la Información, la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC recomendó articular la Política en mención teniendo en cuenta la actualización de la versión 2022 de la NTC-ISO/IEC 27001 incluyendo buenas prácticas de seguridad digital para el manejo de los sistemas y tecnologías de información en la entidad y medidas de seguridad y privacidad efectivas para garantizar la integridad, confidencialidad, privacidad y disponibilidad de la información, lo que permite prevenir y gestionar riesgos asociados al uso del ciberespacio, la inteligencia artificial y de las herramientas tecnológicas en el cumplimiento de los objetivos de la entidad.

Por todo lo anterior, la OTIC, y dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualiza el Plan de seguridad y privacidad de la información al interior del Instituto.

www.ins.gov.co
@INSColombia @insaludcolombia Instituto Nacional de Salud de Colombia
Avenida Calle 26 # 51 - 20 / Bogotá D.C. - Colombia PBX: (601) 220 77 00 / exts. 1101 - 1214 contactenos@ins.gov.co

2. MARCO NORMATIVO

A continuación, se referencian las normas y leyes colombianas que aplican en el ámbito de Seguridad y Privacidad de la información; si cualquier disposición de estas condiciones pierde validez por cualquier razón, todas las demás conservan su fuerza obligatoria:

Constitución Política de Colombia

- **Artículos** 15, 20, 23 y 74.

Leyes

- **Ley 23 de 1982.** Sobre derechos de autor
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1450 de 2011.** Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Ley 1753 de 2015.** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”.
- **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 2052 de 2020.** Por medio de la cual se expide el código general disciplinario.
- **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 2088 de 2021.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones.

Decretos

- **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.
- **Decreto 884 de 2012.** por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **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 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 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 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 1068 de 2015.** por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 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 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto

1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **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 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- **Decreto 338 de 2022.** Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 767 de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Resoluciones

- **Resolución 1519 de 2020.** “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **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
- **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 460 de 2022.** Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- **Resolución 02277 DE 2025.** Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

- **Resolución 1457 de 2025.** Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025.
- **Resolución 0457 de 2020.** Por medio de la cual se adiciona el anexo No. 02 de la Resolución 1607 de 2014 y se actualiza la Política de Tratamiento de Datos Personales del INS.

Otras

- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020**. Confianza y Seguridad Digital
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.
- **CONPES 4144 de 2025.** Política nacional de Inteligencia Artificial
- **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.
- **Directiva Presidencial 02 de 2022.** Reiteración de la política pública en materia de seguridad digital.

3. OBJETIVO

Establecer un marco de acción para continuar implementando el Modelo de Seguridad y Privacidad de la información del INS, que permita la protección de los activos de información que soportan la prestación de servicios digitales de la entidad, logrando fortalecer la confianza de sus funcionarios, ciudadanos, usuarios, proveedores y demás partes interesadas.

4. ALCANCE

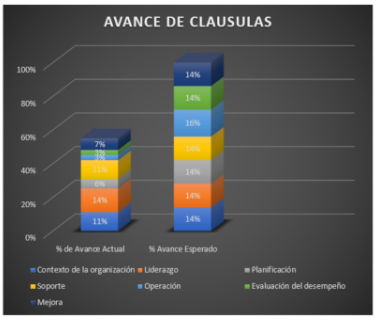
El presente plan, es la hoja de ruta para la vigencia 2026 del INS, y su planeación se enfocará en fortalecer la implementación de actividades de acuerdo con los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados al cumplimiento de las acciones en Seguridad y Privacidad de la información y seguridad digital, contemplando las capacidades y recursos disponibles, para mejorar la confianza de sus funcionarios, ciudadanos, usuarios, proveedores y demás partes interesadas.

5. DIAGNÓSTICO DE NECESIDADES

A partir del autodiagnóstico realizado en la entidad, se evidenciaron brechas en la gestión de la seguridad y privacidad de la información y seguridad digital, las cuales representan riesgos para la protección de la información, la evaluación en la efectividad de los controles y numerales de la Norma ISO 27001:2022 fue la siguiente:

AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA)

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	11%	14%
		Liderazgo	14%	14%
		Planificación	6%	14%
		Soporte	11%	14%
	Implementación	Operación	3%	16%
	Evaluación de Desempeño	Evaluación del desempeño	3%	14%
	Mejora Continua	Mejora	7%	14%
TOTAL			55%	100%



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

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	70	100	GESTIONADO
A.6	CONTROLES DE PERSONAS	90	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	79	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	69	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		77	100	GESTIONADO

Por lo anterior, se hace indispensable la formulación e implementación de un Plan Estratégico de Seguridad y Privacidad de la Información, que permita:

- Definir lineamientos y políticas institucionales alineadas con estándares internacionales y normatividad vigente.
- Establecer controles técnicos y administrativos para mitigar riesgos de seguridad digital.
- Fortalecer la cultura organizacional mediante capacitación y sensibilización.
- Garantizar la continuidad de la operación de los servicios y la protección de la información frente a amenazas internas y externas.

Este plan será la base para consolidar un sistema de gestión integral que asegure la protección de la información como activo crítico de la entidad, contribuyendo a la transparencia, la confianza y la eficiencia en la prestación de los servicios.

6. DESARROLLO DEL PLAN

6.1 Política general de seguridad y privacidad de la información y seguridad digital

Los sujetos obligados deberán preservar y administrar la integridad, confidencialidad, disponibilidad, privacidad, legalidad y confiablidad de la información digital y física, que se produce en el marco de la operación de sus procesos misionales y/o contractuales, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo la prestación ininterrumpida de los servicios científicos, técnicos y de salud pública del INS, con calidad, transparencia, responsabilidad y respetando las disposiciones vigentes en materia de tratamiento de datos personales, en beneficio de la ciudadanía, el sistema de salud y las instituciones que conforman el Sistema Nacional de Ciencia, Tecnología e innovación.

6.2 Objetivos específicos de la política de seguridad y privacidad de la información y seguridad digital del INS.

- Establecer mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, imparcialidad, disponibilidad, privacidad, legalidad y confiabilidad de la información del INS.
- Mitigar el impacto de los incidentes de seguridad y privacidad de la información y seguridad digital en el INS.
- Gestionar los riesgos de seguridad y privacidad de la información y de seguridad digital.
- Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del sistema de gestión de seguridad y privacidad de la información.

www.ins.gov.co
@INSColombia @insaludcolombia Instituto Nacional de Salud de Colombia
Avenida Calle 26 # 51 - 20 / Bogotá D.C. - Colombia PBX: (601) 220 77 00 / exts. 1101 - 1214 contactenos@ins.gov.co

- Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
- Definir y operar la continuidad de la operación de los servicios tecnológicos del INS.
- Garantizar el acceso libre a la ciudadanía de la información pública en poder de la entidad, con el fin de garantizar el cumplimiento del derecho de acceso a la información pública nacional.

El Instituto Nacional de Salud ha actualizado la política de seguridad y privacidad de la información, como parte de su Sistema Integrado de Gestión, y para lograr su implementación y fortalecimiento ha diseñado un conjunto de actividades que dan cumplimiento a las políticas públicas de gobierno y seguridad digital.

El logro de los objetivos específicos de la política de seguridad y privacidad de la información definidos en el presente documento, requiere la definición de actividades detalladas categorizadas según el ámbito de ejecución en la siguiente estructura de plan de trabajo. A continuación, se presenta el plan para fortalecer la implementación del modelo de seguridad y privacidad en el INS para la vigencia 2026, el cual se le hará seguimiento a través del plan de acción institucional:

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
Gestión Activos de información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información tecnológicos	Referente de Seguridad y Privacidad de la Información de la OTIC Coordinador/a de Gestión Documental	2-feb-26	31-mar-26
		Acompañar en la Identificación y/o actualización de los activos de	Enlace de cada proceso	06-jul-26	30-sep-26

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		información en cada proceso de la Entidad	Referente de Seguridad y Privacidad de la Información de la OTIC Coordinador/a de Gestión Documental		
	Consolidar los Activos de Información	Solicitar la aceptación de los activos de información por cada líder de proceso y comité institucional de gestión y desempeño	Enlace de cada proceso Referente de Seguridad y Privacidad de la Información Coordinador/a de Gestión Documental	06-jul-26	30-sep-26
		Consolidar el instrumento de activos de Información de la Entidad.	Referente de Seguridad y Privacidad de la Información Coordinador/a de Gestión Documental	06-jul-26	30-sep-26
	Publicar los Instrumentos de información pública - Ley 1712 de 2014	Actualizar y aprobar por el comité institucional de gestión y desempeño y publicar los instrumentos de información pública: Registro	Referente de Seguridad y Privacidad de la Información Coordinador/a de Gestión Documental	5-oct-26	23-dic-26

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		Activos de Información y el índice de información Clasificada y Reservada.	Comité Institucional de Gestión y Desempeño		
Gestión de Incidentes de Seguridad y Privacidad de la Información y Seguridad Digital	Publicar y socializar el procedimiento de incidentes de seguridad de la información	Actualizar el procedimiento de incidentes de seguridad y privacidad de la información	Referente de Seguridad y Privacidad de la Información	2-feb-26	31-mar-26
	Gestionar los incidentes de seguridad de la información identificados	Realizar seguimiento a los incidentes de seguridad y privacidad de la información y seguridad digital reportados a la mesa de servicio y canales disponibles de acuerdo con lo establecido en el procedimiento definido	Referente de Seguridad y Privacidad de la Información	01-ene-26	31-dic-26
	Gestionar reportes con el CSIRT – GOBIERNO y CSIRT - SALUD	Gestionar los reportes de seguridad producto de los monitoreos a la infraestructura tecnológica y sistemas de	Referente de Seguridad y Privacidad de la Información Líderes de servicios tecnológicos y	02-feb-26	23-dic-26

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		información, así como reportar incidentes mayores o catastróficos al CSIRT Gobierno	de las aplicaciones.		
Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el programa de cambio y cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Actualizar la documentación del programa de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital.	Referente de Seguridad y Privacidad de la Información	2-feb-26	31-mar-26
	Ejecutar el programa de cambio, Cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Implementar y medir las estrategias del programa de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Referente de Seguridad y Privacidad de la Información, Enlaces de procesos	2-feb-26	23-dic-26
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Actualizar y publicar la matriz de verificación de requisitos legales de Seguridad y Privacidad de la Información	Elaborar y publicar la matriz y solicitar las evidencias del cumplimiento de los requisitos legales de Seguridad y Privacidad de la Información.	Referente de Seguridad y Privacidad de la Información Todos los procesos	6-abr-26	23-dic-26

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
Plan de Continuidad de la operación de los servicios tecnológicos	Realizar pruebas de continuidad de la operación de los servicios	Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos	Línea de Infraestructura tecnológica – Gestor de bases de datos	19-ene-26	31-mar-26
Planeación Documental	Revisión y actualización de la documentación estratégica de seguridad y privacidad de la información y seguridad digital	Crear y/o actualizar los manuales, políticas, resoluciones, y demás documentación estratégica del Sistema de Gestión de Seguridad y privacidad de la Información.	Referente de Seguridad y Privacidad de la Información.	01-nov-25	31-ene-26
Gobierno Digital	Implementar los lineamientos de la política	Actualizar el documento de autodiagnóstico de la entidad	Referente de Seguridad y Privacidad de la Información	02-feb-26	23-dic-26

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
	pública de Gobierno y Seguridad Digital que le apliquen al dominio de seguridad y privacidad de la información	Revisar e implementar los lineamientos que define el FURAG en cuanto a las políticas de Gobierno Digital y Seguridad Digital.	Oficial de Seguridad y Privacidad de la Información	02-feb-26	23-dic-26
	CCOCI	Identificar la infraestructura crítica cibernética de la Entidad	Referente de Seguridad y Privacidad de la Información Líderes líneas de infraestructura tecnológica y sistemas de información	02-feb-26	23-dic-26
Revisión de los controles de la norma ISO 27001	Revisión de los controles de la norma ISO 27001:2022	Realizar seguimiento de los controles de Seguridad y Privacidad de la Información y Seguridad Digital	Referente de Seguridad y Privacidad de la Información Líderes de procesos	02-feb-26	23-dic-26
Indicadores SGSI	Crear y realizar seguimiento a los indicadores de medición del SGSPI	Formular, Implementar y alimentar los indicadores del SGSPI	Referente de Seguridad y Privacidad de la Información	02-feb-26	23-dic-24
Gestión de datos personales	Registro de las bases de datos	Registrar y/o actualizar las bases de datos en el aplicativo	Referente de Seguridad y	02-feb-26	23-dic-26

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		RNBD de la SIC, teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Privacidad de la Información		

7. DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

Para efectos de ejecución del Plan de Seguridad y Privacidad de la Información para el INS, se han presupuestado e incluido en el Plan Anual de Adquisiciones los siguientes conceptos:

DEPENDENCIA	TIPO OBJETIVO	PRODUCTO
Inversiones y contratación de servicios especializados		
OTIC	1400-003	Renovar el licenciamiento y soporte del equipo de seguridad perimetral
OTIC	1400-005	Renovar el licenciamiento de monitoreo de infraestructura TI.
OTIC	1400-009	Contratar los servicios de colocation para la infraestructura del INS
Talento Humano		
OTIC	1400-031	Contrato prestación de servicios profesionales al INS
OTIC	1400-032	Contrato prestación de servicios profesionales al INS
OTIC	1400-056	Contrato prestación de servicios profesionales al INS

8. INDICADORES

Para efectos de medición de estas actividades se tendrá en cuenta la escala de calificación y cumplimiento recomendada por el MinTIC en su herramienta de autoevaluación, para disminuir los sesgos de percepción tanto del ejecutor como del evaluador, respecto a la gestión en cada una de ellas.

Esta escala corresponde a:

CALIFICACIONES		
CALIFICACIÓN	**DESCRIPCIÓN**	**VALOR**
NULO	Casi inexistente la aplicación de la actividad del plan en el proceso. No se ha realizado la actividad.	**0**
MUY BAJO	Apenas se reconoce la actividad del plan, pero se aplica muy poco y se deben hacer planes de mejora. La actividad apenas se está iniciando.	**1**
BAJO	Se reconoce la actividad del plan, pero su aplicación es poca en el proceso y se debe reforzar. Se ha iniciado la actividad en su fase de planeación.	**2**
MEDIO	Se reconoce y se aplica la actividad del plan en buena parte de los ejes, pero tiene muchas oportunidades de mejora. La actividad apenas está en ejecución.	**3**
BUENO	Se reconoce y aplica la actividad del plan en la mayoría de los ejes y de buena forma, aún hay oportunidades de mejorar. La actividad está en revisión y ajustes finales.	**4**
EXCELENTE	Reconocimiento, entendimiento y aplicación optima de las metodologías y técnicas asociadas a la actividad del plan en el proceso. La actividad se cumplió satisfactoriamente.	**5**

Valores definidos para la calificación de las actividades del plan.

Por lo anterior, se definen las siguientes metas de cumplimiento:

Métricas del Plan	
Descripción	**Meta Esperada**
Total de tareas del plan = 19 tareas ejecutadas	Puntaje ideal (**todo Excelente**) = 100 Puntos

www.ins.gov.co
@INSColombia @insaludcolombia Instituto Nacional de Salud de Colombia
Avenida Calle 26 # 51 - 20 / Bogotá D.C. - Colombia PBX: (601) 220 77 00 / exts. 1101 - 1214 contactenos@ins.gov.co

Métricas del Plan	
Descripción	**Meta Esperada**
Meta **optimista** esperada para la vigencia = 17 tareas ejecutadas	Puntaje **Excelente** = 90 puntos
Meta **realista** esperada para la vigencia = 15 tareas ejecutadas	Puntaje **Bueno** = 60 puntos
Meta **tolerable** para el periodo = 10 tareas ejecutadas	Puntaje **Aceptable** = 40 puntos

Metas estimadas para el plan para la vigencia 2026.

9. HOJA DE RUTA DE IMPLEMENTACIÓN DEL PLAN

Ver hoja de ruta del plan

10. CONTROL DE CAMBIOS.

Versión	Fecha de actualización			Descripción de los cambios
	aaaa	mm	dd	
1.0	2022	12	28	Versión inicial del documento
2.0	2024	01	12	Actualización 2024
3.0	2024	12	28	Actualización 2025
4.0	2025	07	04	Actualización 2025
5.0	2025	12	30	Actualización 2026

www.ins.gov.co
@INSColombia @insaludcolombia Instituto Nacional de Salud de Colombia
Avenida Calle 26 # 51 - 20 / Bogotá D.C. - Colombia PBX: (601) 220 77 00 / exts. 1101 - 1214 contactenos@ins.gov.co

Salud | Instituto Nacional de Salud

HOJA DE RUTA PLANES INSTITUCIONALES

Recomendación general: Diligenciar en minúscula, revisar escritura y ortografía antes de enviar, con la pestaña revisar y ortografía.

FECHA DE DILIGENCIAMIENTO	29/12/25	NOMBRE DE QUIEN DILIGENCIA	SERGIO ANDRÉS RAMOS PAHUANA

CÓDIGO DE LA ACTIVIDAD/TAREA DEL PLAN DE ACCIÓN ASOCIADO	NOMBRE DEL PLAN	CATEGORIA/COMPONENTE/PRODUCTO	SUBCATEGORIA/SUBCOMPONENTE/ACCIÓN ESTRATÉGICA	TAREA	ENTREGABLE	PROCESO RESPONSABLE	LÍDER DEL PROCESO	RESPONSABLE DEL REPORTE DE LA TAREA	META TOTAL	UNIDAD META AVANCE FÍSICO	FUNCIÓN PARA CALCULAR EL AVANCE DE LA META	FRECUENCIA DE MEDICIÓN DE AVANCE	METAS FÍSICAS PARCIALES	FECHA INICIO	FECHA FINALIZACIÓN
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión Activos de información	N/A	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información tecnológicos	Documentos creados y/o actualizados	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2/02/26	31/03/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión Activos de información	N/A	Acompañar en la Identificación y/o actualización de los activos de información en cada proceso de la Entidad	Herramienta de levantamiento del inventario de activos de información Actas de trabajo	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	6-jul-26	30/09/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión Activos de información	N/A	Solicitar la aceptación de los activos de información por cada líder de proceso y comité institucional de gestión y desempeño	Correo solicitud de aceptación de los activos de información Acta de comité	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	6-jul-26	30/09/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión Activos de información	N/A	Consolidar el instrumento de activos de Informació de la Entidad	Herramienta con el consolidado del inventario de activos de información	GESTIÓN DOCUMENTAL	Kerim Tatiana Castillo Agudelo	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	6-jul-26	30/09/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión Activos de información	N/A	Actualizar y aprobar por el comité institucional de gestión y desempeño y publicar los instrumentos de información pública: Registro Activos de Información y el índice de información Clasificada y Reservada.	Instrumento del RAI y del Índice de información clasificada y reservada Acta de comité	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	5-oct-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión de Incidentes de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Actualizar el procedimiento de incidentes de seguridad y privacidad de la información y seguriad digital	Documentos creados y/o actualizados	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2-feb-26	31/03/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión de Incidentes de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Realizar seguimiento a los incidentes de seguridad y privacidad de la información y seguridad digital reportados a la mesa de servicio y canales disponibles de acuerdo con lo establecido en el procedimiento definido	Correos electrónicos Informes de seguimiento	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	1-ene-26	31/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión de Incidentes de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Gestionar los reportes de seguridad producto de los monitoreos a la infraestructura tecnológica y sistemas de información, así como reportar incidentes mayores o catastróficos al CSIRT Gobierno	Informes de seguimiento Informe de reporte de incidentes (en el caso de presentarse)	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	2-feb-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Actualizar la documentación del programa de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital.	Documentos creados y/o actualizados	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2-feb-26	31/03/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Implementar las estrategias del programa de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Material Multimedia Listados de asistencia	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	12	NÚMERO	SUMA	MENSUAL	N/A	2-feb-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Matriz de verificación de Requisitos Legales de Seguridad de la Información	N/A	Elaborar, publicar la matriz y solicitar las evidencias del cumplimiento de los requisitos legales de Seguridad y Privacidad de la Información y seguridad digital	Matriz de requisitos legales	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	6-abr-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Plan de Continuidad de la operación de los servicios tecnológicos	N/A	Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos	Informe de las pruebas realizadas	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	2	NÚMERO	SUMA	SEMESTRAL	N/A	19-ene-26	31/03/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Planeación Documental	N/A	Crear y/o actualizar los manuales, políticas, resoluciones, y demás documentación estratégica del Sistema de Gestión de Seguridad y privacidad de la Información, alineándolos al MSPI.	Documentos creados y/o actualizados	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	1-nov-25	31/01/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gobierno y Seguridad Digital	N/A	Actualizar el documento de autodiagnóstico de la entidad	Herramienta de autodiagnóstico del MSPI	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2-feb-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gobierno y Seguridad Digital	N/A	Revisar e implementar los lineamientos que define el FURAG en cuanto a las políticas de Gobierno Digital y Seguridad Digital.	Herramienta del FURAG	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2-feb-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gobierno y Seguridad Digital	N/A	Identificar la infraestructura crítica cibernética de la Entidad	Heramienta de identificación de infraestructura crítica cibernética	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2-feb-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Revisión de los controles de la norma ISO 27001	N/A	Realizar seguimiento de los controles de Seguridad y Privacidad de la Información y Seguridad Digital	Heramienta de seguimiento de controles	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	2-feb-26	23/12/26
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Indicadores SGSI	N/A	Formular, implementar y alimentar los indicadores del Sistema de Gestión de Seguridad y Privacidad de la Información	Fichas técnicas de indicadores	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	2-feb-26	23/12/24
140114/140143	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión de datos personales	N/A	Registrar y/o actualizar las bases de datos en el aplicativo RNBD de la SIC, teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Certificado emitido por el RNBD	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2-feb-26	23/12/26