PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

2025

Control de Versiones

Versión	Fecha	Modificación
1.0	Diciembre 28 2022	Versión inicial del documento
2.0	Enero 12 2024	Actualización 2024
3.0	Diciembre 28 de 2024	Actualización 2025

Control de Cambios

	ELABORÓ	REVISÓ	APROBÓ
Instituto Nacional de Salud	Robert Manuel Pulido Castellanos	Amalia Emelda Carrillo Guiza	Heysell Nafasha García Aguilar
	Profesional Contratista OTIC	Profesional Contratista OTIC	Jefe OTIC

Tabla de Contenido

Índice de Tablas

1. INTRODUCCIÓN

El Instituto Nacional de Salud – INS se encuentra comprometido con la Seguridad de la Información, siguiendo los lineamientos establecidos dentro de la Política de Seguridad Digital 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 , a través de la asignación de recursos necesarios para garantizar que los procesos de la Entidad que se apoyan en la infraestructura tecnológica, para que estén siempre disponibles y protegidos contra cualquier ciberataque, de esta manera se puede realizar el cumplimiento de sus objetivos estratégicos.

El Plan Estratégico de Seguridad de la Información (PESI), es un documento de índole estratégico, que tiene como objetivo permitir a las entidades diseñar, planificar y ejecutar sus proyectos de seguridad de la información y así poder implementar el Modelo de Seguridad en un corto , mediano y largo plazo, teniendo en cuenta insumos de diagnóstico que le permitan identificar su estado actual y así poder orientar los objetivos a lograr o las actividades a ejecutar para llegar al punto deseado en cuanto a la implementación de seguridad y privacidad en la entidad

Este documento tiene como fin presentar el Plan Estratégico de Seguridad y Privacidad de la Información del INS, con el fin de garantizar su operación, monitoreo, revisión y mejora continua, evidenciando que el Instituto Nacional de Salud se encuentra comprometido con la Seguridad de la Información.

2. OBJETIVO GENERAL

Presentar el Plan Estratégico de Seguridad de la Información para operar, monitorear, revisar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información del Instituto Nacional de Salud - INS

2.1 Objetivos Específicos

- Presentar actividades a desarrollar en la vigencia 2025, teniendo como base el cumplimiento de los requisitos definidos en la ISO Norma 27001 y el Modelo de Seguridad y Privacidad de la Información - MSPI.
- Presentar actividades distribuidas en los niveles estratégico, táctico y operativo.
- Identificar actividades que se deben ejecutar periódicamente (Actividades de Mantenimiento del SGSI y el Modelo de Seguridad y Privacidad de la Información - MSPI).

3. PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan Estratégico de Seguridad de la Información en el Instituto Nacional de Salud, se desarrollan con base en los resultados del documento de Análisis de Brechas ISO 27001.

Con el fin de entender la estructura de este Plan Estratégico, a continuación, se describen los niveles que le componen:

- **Nivel Estratégico:** Plantea actividades a nivel de toma de decisiones de alta dirección y el compromiso de esta instancia, para que el Sistema de Gestión de Seguridad de la Información en el Instituto Nacional de Salud alcance los objetivos propuestos.

- **Nivel Táctico:** Plantea actividades a nivel de toma de decisiones por parte de gerencias o mandos medios, que tienen como fin alcanzar los objetivos del SGSI planteados a nivel estratégico. Se caracteriza por tener actividades a corto plazo, que descomponen las actividades de nivel estratégico en entregables más pequeños.

- **Nivel Operativo:** Describe la operación diaria del SGSI. Traza una hoja de ruta para lograr los objetivos tácticos dentro de un plazo realista. Es detallado y hace énfasis en los objetivos a corto plazo.

A continuación, se establecen los responsables, del Plan Estratégico de Seguridad de la Información en el Instituto Nacional de Salud - INS:

- **Comité de Alta Dirección:** La Alta Dirección del Instituto Nacional de Salud, como la máxima autoridad para la toma de decisiones sobre el SGSI.
- **Responsable del Sistema de Seguridad de la Información:** Como responsable de la gestión general del SGSI.
- **Ingeniero de Seguridad de la Información:** Como el desarrollador de la documentación necesaria para la implementación y operación del SGSI.
- **Oficina de Tecnologías de la Información:** Como ejecutor de los controles tecnológicos.

3.1 Descripción detallada del cronograma de las actividades a realizar en el Año 2025

A continuación, en las tablas 1, 2 y 3 se describen las actividades a Nivel Estratégico, Táctico y Operativo para ejecución del 2025.

Tabla 1 Descripción de actividades Nivel Estratégico para el año 2025

Descripción de Actividades para el Año 2025				
Nivel Estratégico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Revisar los resultados del SGSI por la Dirección.	Realizar la Revisión del Sistema de Gestión de Seguridad de la Información del INS por parte del Comité de Seguridad de la Información semestralmente o cuando ocurran cambios significativos, para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el SGSI son evidentes.	Oficina de Tecnologías de la Información	Febrero
	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI e identificar las oportunidades de mejora.	Realizar la revisión de los Diagnósticos de Sistema de Gestión de Seguridad de la Información del INS, con la finalidad de evaluar si se logró el nivel de madurez propuesto y revisar las estrategias para cumplir las metas definidas	Oficina de Tecnologías de la Información	Marzo
	Revisión y actualización de políticas, objetivos y métricas del SGSI, así como los requisitos de las partes interesadas.	Actualizar objetivos, políticas, procedimientos y métricas del SGSI, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, y riesgos identificados.	Oficina de Tecnologías de la Información	Abril
	Evaluar acciones correctivas originadas en la revisión por la dirección y en las auditorías internas al SGSI	Evaluar e identificar acciones correctivas adecuadas con base en lecciones aprendidas, las originadas en la revisión por la dirección y las establecidas de acuerdo con las auditorías realizadas a nivel interno las cuales pudieran haber impactado sobre la efectividad o el rendimiento del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Agosto
	Definir el Portafolio de Proyectos del SGSI para el siguiente año.	Proponer y planear los proyectos futuros que fortalezcan la implementación y operación del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información del INS	Noviembre
	Garantizar presupuesto del SGSI para el siguiente año.	Definir y contar con presupuesto adecuado de acuerdo con los proyectos definidos para garantizar la operación y mejora continua del Sistema de Gestión de Seguridad de la Información del INS.	Oficina de Tecnologías de la Información	Diciembre

Fuente Propia INS

Tabla 2 Descripción de actividades Nivel Táctico para el año 2025

Descripción de Actividades para el Año 2025				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Revisar las políticas específicas y los procedimientos de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y garantizar su aplicación.	Actualización de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.	Oficina de Tecnologías de la Información	Febrero
	Medir los indicadores definidos del SGSI.	Medir los indicadores definidos en el SGSI con el fin de monitorear la eficacia de los controles o grupos de controles definidos para el Sistema de Gestión de Seguridad de la Información del INS.	Responsable de Seguridad de la Información	Mayo
	Dar a conocer las políticas y procedimientos de seguridad de la información al interior del INS.	Dar a conocer las políticas de seguridad de la información a todos los interesados del INS y garantizar que las mismas estén implementadas. Esta sensibilización debería realizarse mínimo una vez al año.	Responsable de Seguridad de la Información	Junio y Diciembre
	Aprobar los riesgos residuales de seguridad de la información.	Aprobar los riesgos residuales luego del establecimiento de los controles de los riesgos del INS.	Oficina de Tecnologías de la Información	Junio
	Revisar las políticas específicas y los procedimientos de seguridad de la información con base en las mejores prácticas Anexo A ISO27001 y garantizar su aplicación.	Actualización de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.	Oficina de Tecnologías de la Información	Febrero
	Medir los indicadores definidos del SGSI.	Medir los indicadores definidos en el SGSI con el fin de monitorear la eficacia de los controles o grupos de controles definidos para el Sistema de Gestión de Seguridad de la Información del INS.	Responsable de Seguridad de la Información	Mayo
	Dar a conocer las políticas y procedimientos de seguridad de la información al interior del INS.	Dar a conocer las políticas de seguridad de la información a todos los interesados del INS y garantizar que las mismas estén implementadas. Esta sensibilización debería realizarse mínimo una vez al año.	Responsable de Seguridad de la Información	Junio y Diciembre
	Aprobar los riesgos residuales de seguridad de la información.	Aprobar los riesgos residuales luego del establecimiento de los controles de los riesgos del INS.	Oficina de Tecnologías de la Información	Junio

Descripción de Actividades para el Año 2025				
Nivel Táctico	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Aprobar los planes de tratamiento identificados.	Aprobar los planes de tratamiento identificados para los riesgos residuales de seguridad de la información.	Oficina de Tecnologías de la Información	Agosto
	Definir y llevar a cabo pruebas al plan de continuidad y al DRP	Ejecutar las pruebas definidas en el plan de continuidad de negocio y el plan de recuperación de desastres tecnológicos en el entendido de que ocurra una interrupción que inhabilite las operaciones del INS verificando que los procesos se puedan recuperar a nivel operativo y tecnológico como: datos, hardware y software críticos.	Responsable de Seguridad de la Información	Noviembre

Fuente: Propia INS

Tabla 3 Descripción de actividades Nivel Operativo para el año 2025

Descripción de Actividades para el Año 2025				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Actualizar el inventario de activos y contenedores de información.	Mantener actualizado el inventario de activos y riesgos de seguridad de la información y su correspondiente valoración.	Ing. De seguridad de la información del INS	Mayo
	Llevar a cabo análisis de riesgos de seguridad de la información con los diferentes procesos del INS	Realizar la identificación de los activos de información y Datos Personales, que están dentro del alcance del Sistema de Gestión de Seguridad de la Información. Así como evaluar los riesgos de seguridad de la información que afecten la confidencialidad, integridad o disponibilidad de la información.	Ing. De seguridad de la información del INS	Mayo
	Realizar campañas de sensibilización y concienciación.	Dar capacitaciones y concientizar a todo el personal del INS y los terceros involucrados, a los que se le asignen responsabilidades definidas en el SGSI y verificar que estén suficientemente capacitados. Asegurando que todo el personal esté concientizado de la importancia de la seguridad de la información y de cómo contribuye a la consecución de los objetivos del Sistema de Gestión de Seguridad de la Información del INS.	Responsable de la Seguridad de la Información	Mayo
	Definir planes de tratamiento para los riesgos residuales de seguridad de la información no tolerables	Plantear y ejecutar planes de tratamiento que identifiquen las acciones, los recursos, las responsabilidades y las prioridades para gestionar los riesgos residuales no tolerables de seguridad de la información.	Ing. De seguridad de la información del INS	Julio

Descripción de Actividades para el Año 2025				
Nivel Operativo	**Actividad**	**Descripción**	**Responsable**	**Terminación Estimada**
	Actividades de mantenimiento			
	Implementar y monitorear los planes de tratamiento para los riesgos residuales definidos.	Ejecutar y hacer seguimiento a las acciones identificadas, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información.	Responsable de Seguridad de la Información	Agosto
	Llevar a cabo análisis vulnerabilidades y hacer seguimiento a la remediación.	Realizar la planeación y ejecución de Análisis de Vulnerabilidades a los sistemas de información y servicios tecnológicos críticos de la Entidad de manera periódica.	Ing. De seguridad de la información del INS	Agosto
	Llevar a cabo pruebas de ingeniería social.	Realizar la planeación y ejecución de pruebas de ingeniería social de acuerdo con las acciones a tomar en caminadas al cumplimiento del manual y la política de seguridad de la información del Instituto Nacional de Salud	Ing. De seguridad de la información del INS	Noviembre
	Realizar Auditorías al SGSI.	Llevar a cabo auditorías al Sistema de Gestión de Seguridad de la Información del INS, para identificar oportunidades de mejora.	Responsable de la Seguridad de la Información	Septiembre
	Reporte de eventos e incidentes de seguridad de la información.	Identificar brechas, detectar y prevenir eventos e incidentes de seguridad de la información.	Responsable de la Seguridad de la Información	bimensual

Fuente: Propia INS

4. GLOSARIO

Activo de información: Sustenta uno o más procesos de negocio. En otras palabras, es todo aquello que tiene valor para la organización.

Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias calificándolas y evaluándolos a fin de determinar la capacidad de la Entidad para su aceptación y manejo.

Acceso a la Información Pública Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.

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 Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. En otras palabras, es todo aquello que tiene valor para la organización. 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.

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.

La Autenticidad, esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser.

BIA: Business Impact Analysis (Análisis de Impacto al Negocio): El proceso de análisis de las funciones de negocio y el efecto que una interrupción del negocio podría tener sobre ellos.

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)
Confidencialidad: Propiedad que determina que la información no está disponible ni sea revelada a individuos, Entidades o procesos no autorizados.

Continuidad del Negocio: Describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.

Contenedor: Cualquier componente (sea humano, tecnológico, software, etc.) que contenga uno o más activos de información.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.

Evento de seguridad de la información Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

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).

Gestión del riesgo: La gestión del riesgo se refiere a los principios y metodología para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodología a riesgos particulares.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

MTPD: (Maximum Tolerable Period of Disruption) Periodo Máximo Tolerable de interrupción.

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.

Plan de Continuidad del Negocio: (o sus siglas en inglés **BCP**, por Business Continuity Plan) es un plan logístico de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.
Plan de Recuperación de Desastres (DRP): Conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los servicios informáticos.

Plan de tratamiento de riesgos Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Riesgo residual: Nivel restante del riesgo después del tratamiento del riesgo.

Seguridad de la Información Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como, autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de Gestión de Seguridad de la Información Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la Seguridad de la Información.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. HOJA DE RUTA

Para seguimiento, control y ejecución del Plan de Seguridad y Privacidad de la Información PESI se encuentra articulada y alineada con los Planes, Directrices y Sistema de Gestión de Calidad del INS, como se relacionan a continuación:

- **Plan de Acción**, define los indicadores de gestión, ejecución financiera, y el cronograma con su respectivo seguimiento al avance de ejecución y cumplimiento de objetivos, proyectos, actividades y tareas definidas para el año 2025.

- **Matriz Caracterización del Riesgo**, identifica, clasifica y estructura los riesgos por categorías, tales como: operativos, relacionados con usuarios, productos, prácticas y procesos administrativos.

- **Plan Anual de Adquisiciones de Bienes y Servicios**, establece la planificación y ejecución presupuestal asignada a la Oficina TIC para garantizar la disponibilidad y ejecución de los recursos necesarios.

- **PETI,** constituye una guía clara y precisa para la gestión estratégica de las TIC en el INS, estableciendo prioridades y objetivos para el periodo 2023-2026.

6. BIBLIOGRAFÍA

- Norma ISO 27001:2013: Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (SGSI). Requisitos.
- Norma ISO/IEC 27032:2012. Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad.
- Constitución Política de Colombia. Artículo 15, 209 y 269.
- 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.
- 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 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- 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 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.