PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE SALUD - INS

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - OTIC

2025

Control de Versiones

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

Control de Cambios

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

Tabla de contenido

Tabla de Ilustraciones

Lista Tablas

1. INTRODUCCIÓN

Las tendencias tecnológicas de los últimos años han permitido crear de manera exponencial cantidades de información, cambiando la manera de ver las cosas por parte de todos aquellos quienes tienen acceso a esta. Particularmente en las entidades de la administración pública, se hace necesario contar con la conciencia del poder de la información, el alcance que tiene la misma y principalmente la entrega de esta de manera oportuna y eficiente a la ciudadanía.

En este contexto, bajo la perspectiva de tener información disponible en activos de información vulnerables, surge la necesidad de establecer lineamientos que permitan una adecuada administración del riesgo, integrándola como parte del Instituto Nacional de Salud - INS. Este proceso involucra actividades de identificar, analizar, controlar y mitigar los riesgos de seguridad de la información que podrían afectar negativamente el logro de los objetivos estratégicos de la Entidad.

En este sentido, el presente documento se convierte en una necesidad casi imperativa, dado que la materialización de los riesgos de seguridad de la información puede obstaculizar el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales tanto internos como los dirigidos a la ciudadanía, para los cuales fue concebida la Entidad.

Desde esta perspectiva, la gestión de los Riesgos de Seguridad de la Información se presenta como una herramienta vital para el desarrollo, implementación y mejora continua de la Entidad frente a la prestación de servicio y la entrega de información, partiendo de la protección del valor de la organización a partir de la seguridad de la información, tanto física como digital.

Al tener una visión clara de los riesgos que pueden afectar la seguridad de la información, la entidad puede establecer controles y medidas efectivas, viables y transversales, con el propósito de preservar la disponibilidad, integridad y confidencialidad de su información. Para lograrlo, es esencial definir los lineamientos que se deben seguir para el análisis y evaluación de los riesgos de Seguridad de la Información de la Entidad. Todo esto, cumplimiento con la normativa establecida por el estado Colombiano y adoptando las buenas prácticas y los lineamientos de los estándares que sirven como guía.

2. OBJETIVOS

Objetivo General

Analizar los Riesgos de seguridad de la Información, definiendo las líneas de acción y actividades del Plan de Tratamiento, para mitigar los riesgos y salvaguardar la integridad, disponibilidad y confidencialidad de la información del Instituto Nacional de Salud - INS.

Objetivos Específicos

a. Definir un cronograma de actividades que permita la administración y gestión de los riesgos de la entidad a nivel de seguridad de la información.

b. Establecer y ejecutar lineamientos y actividades puntuales para el tratamiento de los riesgos en el Instituto Nacional de Salud - INS.

c. Establecer controles que permitan minimizar la probabilidad de materialización de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información se desarrolla de acuerdo con lo establecido en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6, lineamiento emitido por la Función Pública[1]. Este documento es el encargado de definir las actividades a llevar a cabo, así como la aplicabilidad y el cumplimiento por parte de los funcionarios, contratistas y terceros que mantengan algún tipo de relación con la entidad.

En ese sentido, el objetivo es establecer las actividades a realizar en el año 2025, centradas en la identificación y análisis de los Riesgos de Seguridad y Privacidad de la Información, junto

[1] Consultar en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

con sus correspondientes controles, este proceso se guía por el ciclo de Demming (PHVA) y se alinea con el cumplimiento de la Política de Seguridad de la Información de la Entidad.

Este tratamiento de riesgo debe buscar abarcar a todos los procesos y actividades llevadas a cabo por la entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales.

4. CONCEPTOS TÉCNICOS

A continuación, se listan los conceptos más importantes y necesarios para la comprensión de la metodología sobre los Riesgos de Seguridad de la Información y establecidos en la Política de Administración de Riesgos que son:

- **Activo**: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Amenazas**: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

- **Análisis del riesgo**: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

- **Apetito de riesgo**: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **CCOC**: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.
- **Capacidad de riesgo**: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno

que no sería posible el logro de los objetivos de la Entidad.

- **Causa**: Factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- **Causa Raíz**: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Consecuencia**: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Confidencialidad**: Propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.

- **Control**: Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Disponibilidad**: Propiedad de ser accesible y utilizable a demanda por la entidad.

- **Factores de Riesgo**: Son las fuentes generadoras de riesgos.

- **Gestión del riesgo**: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **ICC**: Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:** Propiedad de exactitud y completitud.
- **Línea estratégica:** Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de

Coordinación de Control Interno.

- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

- **Política de administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.

- **Primera línea de defensa:** Personas que se encuentras a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.

- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Riesgo de corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo de imagen o reputacional:** Posibilidad de ocurrencia de un evento que afecten la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.

- **Riesgo de Seguridad de la Información**: 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), así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.

- **Riesgos estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización publica y por tanto impactan toda la entidad.

- **Riesgos financieros:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

- **Riesgos gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

- **Riesgo inherente:** Riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

- **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo. El resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Riesgos tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

- **Segunda línea de defensa:** Personas que asisten y guían a la línea estratégica y a

laprimera línea de defensa en la gestión adecuada de los riesgos que pueden afectar elcumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgosde corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

- **Tercera línea de defensa:** Personas que provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.

- **Tolerancia al riesgo:** Preparación de la organización o de la parte involucrada para soportar el riesgo después del tratamiento de este con el fin de lograr sus objetivos.

- **Tratamiento al riesgo:** Respuesta establecida por la primera línea de defensa para lamitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. JUSTIFICACIÓN

La gestión de riesgos se ha convertido en uno de los procesos por excelencia para identificar con la suficiente premura posibles amenazas y, por ende, definir potenciales causas a problemas futuros. En ese sentido, el análisis de estos riesgos permite prever actividades orientadas a mitigar dichas amenazas, con el objetivo de que la materialización del riesgo tenga un impacto mínimo o, en su defecto, contar con un protocolo para actuar ante tales eventualidades.

De esta manera, las entidades buscan ser proactivas y resiliente ante los problemas de su entorno, anticipándose a las problemáticas comunes vinculadas al cumplimiento de sus objetivos misionales. La Información producida en la gestión que realizan las organizaciones en los diversos ámbitos del sector constituye uno de los activos más importantes para las instituciones que participan en su tratamiento.

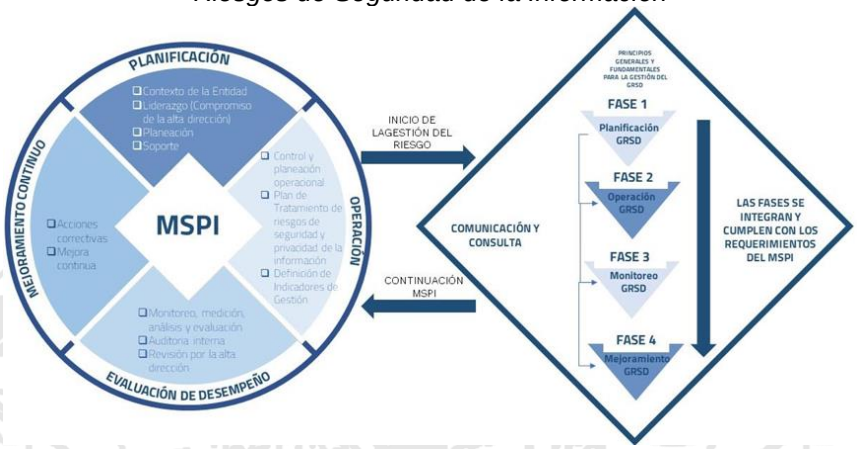
En concordancia con esto, el Gobierno Nacional plantea la Política de Gobierno Digital[2], Que introduce un nuevo enfoque, en este, no solo la Administración Pública, sino también los diferentes actores de la sociedad, como el ciudadano, la empresa privada, entes externos, etc., son elementos fundamentales para el desarrollo integral del gobierno Digital en Colombia, En este contexto, las necesidades y problemáticas del entorno determinan el uso de la tecnología y la manera en que esta puede contribuir a la generación de valor público y aportar a la sociedad.

Dentro de los lineamientos Nacionales tiene presente lo estipulado en el Decreto 1078 de 2015 relacionado a la estrategia de Gobierno Digital, las entidades públicas están obligadas a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), con el objetivo de implementar y hacer uso y apropiación del Sistema de Gestión de Seguridad de la Información al interior de la Entidad.

El MSPI permite la integración en cada una de sus fases, actividades y tareas asociadas a la Gestión de Riesgos de Seguridad de la Información, ya que esta práctica constituye su base fundamental. A continuación, en la Ilustración 1 Acciones MSPI Integrado con el Modelo de Gestión de Riesgos de Seguridad de la Información.

[2] Ministerio de Tecnología y Comunicaciones – MINTIC. Política de Gobierno Digital. Bogota. 2018. En: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/75180:La-nueva-politica-de-Gobierno- Digital-promueve-la-proactividad-y-la-innovacion-ciudadana#:~:text=El%20Ministerio%20de%20Tecnolog%C3%ADas%20de,para%20consolidar%20un%2 0Estado%20y

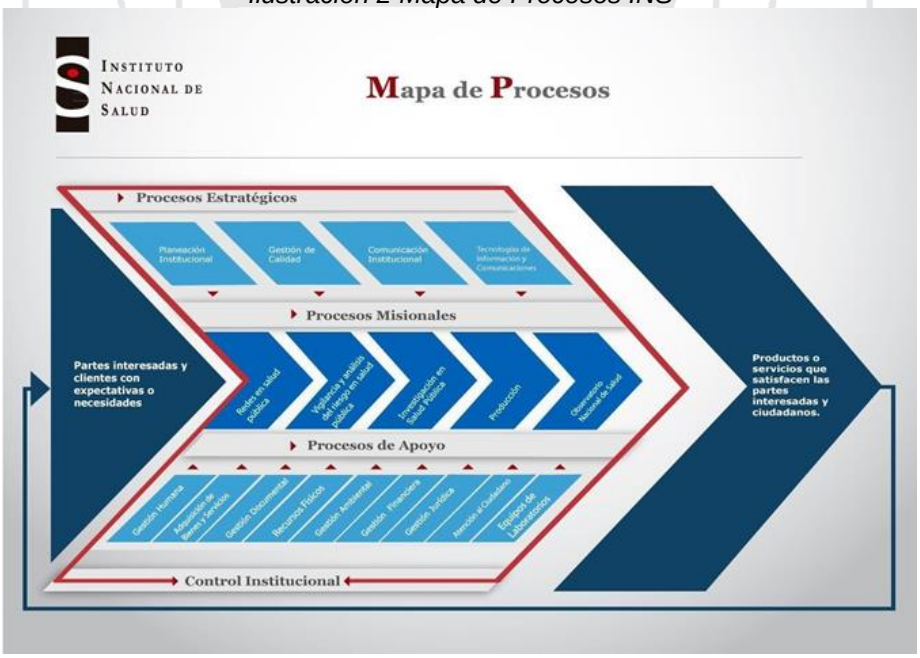
Ilustración 1 Acciones MSPI Integrado con el Modelo de Gestión de Riesgos de Seguridad de la Información



Fuente: Ministerio de Tecnologías de Información y las Comunicaciones

La aplicación del presente plan involucra el mapa de procesos establecido en el InstitutoNacional de Salud INS como se evidencia en la Ilustración 2 Mapa de Procesos INS:

Ilustración 2 Mapa de Procesos INS



Fuente: Propia INS

6. ACTIVIDADES PARA DESARROLLAR

El Plan definido que da cumplimiento a la ejecución de las actividades asociadas al Sistema de Gestión de Seguridad de la Información. A continuación, se detallan las actividades o tareas a realizar durante el año 2025 incorporando, tiempo de ejecución y evidencias como se observa en la Tabla 1 Cronograma de Actividades 2025.

Tabla 1 Cronograma de Actividades 2025

Actividades o Tareas	FECHA DE EJECUCIÓN												Evidencia
	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	
Realizar actualización y monitoreo de Matriz de Riesgos de Seguridad de la Información con cada uno de los procesos													Informe de Monitoreo y Matriz de Riesgos de Seguridad de la Información actualizada.
Programa de formación, alfabetización y concienciación del SGSI para el año 2025.													Informe de jornadas de alfabetización digital y riesgos realizadas.
Generar estrategias internas de ejercicios de ingeniería social.													Informe de Ejercicios realizados y de recomendaciones.
Llevar a Cabo análisis de vulnerabilidades y hacer seguimiento de remediación.													Informe de Análisis de vulnerabilidades para toma de decisiones.
Definir plan de continuidad de negocio y DRP													Documentos base de los planes.
Definición y actualización de la política DLP basada en la herramienta de DLP													Documento Política DLP e informe de implementación de la Política DPL.

Actividades o Tareas	FECHA DE EJECUCIÓN												Evidencia
	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	
Estudio de indicadores para monitorear la efectividad de los Controles													Informe de Indicadores de cumplimiento para cada uno de los controles asociados.

Fuente; Propia INS

7. HOJA DE RUTA

Para seguimiento, control y ejecución del Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información se encuentra articulado y alineado 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.