Plan de Tratamiento de Riesgo 2023

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

Tabla de contenido

Contenido

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

1. INTRODUCCIÓN

Las tendencias tecnológicas de los últimos años han permitido crear de manera exponencial cantidades de información que jamás en la historia de la humanidad se había creado, transportado, transformado o compartido, cambiando la manera de ver las cosas por parte de todos nosotros. 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 la misma de manera oportuna a la ciudadanía.

En este sentido, bajo la perspectiva de tener información disponible en activos de información los cuales son vulnerables, hay una necesidad clara de estructurar lineamientos que permitan realizar una adecuada administración del riesgo que haga parte integral del Instituto Nacional de Salud, cumpliendo las actividades de identificar, analizar, controlar y mitigar los riesgos de seguridad de la información que podrían afectar de manera negativa el logro de los objetivos estratégicos de la Entidad.

En esta dirección, el presente documento se convierte en una necesidad casi imperativa, toda vez que la materialización de los riesgos de seguridad de la información puede impedir 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.

Bajo esa perspectiva, la gestión de riesgos de seguridad de información se presenta como una herramienta importante 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.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

2. OBJETIVOS

Objetivo General

Adelantar la gestión de riesgos de seguridad de la Información del Instituto Nacional de Salud.

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.

3. ALCANCE

El plan de tratamiento de riesgos se desarrolla conforme a lo documentado en la Guía de administración del riesgo, y es dicho documento el que define las actividades a adelantar y los pormenores correspondientes. En ese sentido, se busca establecer las actividades a realizar en el año 2023 para la identificación y análisis de los riesgos de Seguridad y Privacidad de la Información con sus correspondientes controles, orientado por el ciclo de Demming (PHVA) y alineado al cumplimiento de la Política de Seguridad de la Información de la Entidad.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

4. CONCEPTOS TÉCNICOS

- **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).

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

- **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.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

- **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:** Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

- **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.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

- **Riesgos de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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.

- **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.

- **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 la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de 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,

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

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 la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

- **Vulnerabilidad:** Debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

5. JUSTIFICACIÓN

En las últimas dos décadas, la gestión de riesgos se ha convertido en uno de los procesos por excelencia para poder identificar, con la suficiente premura, posibles amenazas y por ende definir potenciales causas a problemas futuros. En ese sentido, el análisis de estos hace que se prevean actividades tendientes a atacar dichas amenazas, con el fin de que la posible materialización de dicho riesgo impacte muy poco o en su defecto se tenga un protocolo para poder actuar ante dichas materializaciones.

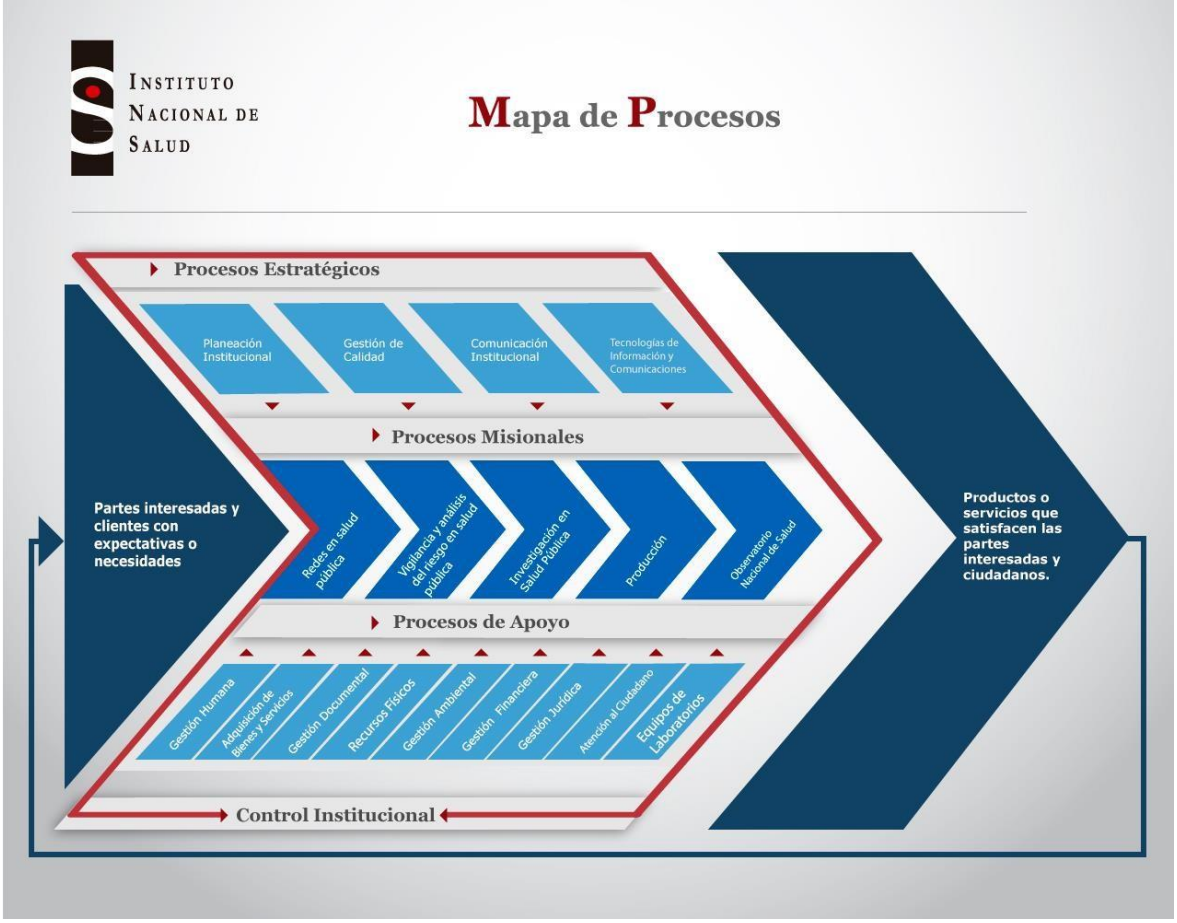
Es así como las Entidades buscan ser proactivas y resilientes ante problemas de su entorno, buscando adelantarse a la problemática comunes del que hacer del cumplimiento de su misionalidad.

En concordancia con esto, el gobierno nacional plantea la política de Gobierno Digital[1], con la cual se genera un nuevo enfoque, en donde no sólo la Administración Pública sino también los diferentes actores de la sociedad tales como el ciudadano, la empresa privada, entes externos, etc., son elementos fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas del contexto, determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público y aporte a la sociedad.

[1] 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%20Estado%20y

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

La aplicación del presente plan involucra el mapa de procesos establecido en el Instituto Nacional de Salud:



Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**

6. ACTIVIDADES A DESARROLLAR

El Plan definido da cumplimiento a las actividades asociadas a la gestión del Sistema de Gestión de Seguridad de la Información.

El detalle de las actividades a realizar, tiempo de ejecución de estas, responsable y participantes, para adelantar la implementación de este plan se definen a continuación.

Actividades o Tareas	FECHA DE EJECUCIÓN												Evidencia
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
Realizar actualización de matriz de riesgo con cada uno de los procesos													Matriz de riesgo actualizada
Realizar actividades de identificación de controles y medidas de protección que permitan la mitigación de los riesgos de seguridad de la información													Matriz de controles asociada en la matriz de riesgo
Estudio de indicadores para monitorear la efectividad de los controles													Indicadores de cumplimiento para cada uno de los controles asociados

Av. Calle 26 No. 51- 20, Bogotá, D.C., Colombia
Conmutador: (1) 220 7700 Ext. 1703-1704
correo electrónico: contactenos@ins.gov.co
Página web: **www.ins.gov.co**