PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024-2026

Superintendencia Nacional de Salud

Área Responsable: Subdirección de Tecnologías de la información

2026 - Enero

Supersalud

Bernardo Armando Camacho Rodríguez - **Superintendente Nacional de Salud**

Rainer Narval Naranjo Charrasquiel - **Secretaría General**

Genaro Ballén Hernández - **Delegatura de Investigaciones Administrativas**

Gustavo Adolfo Flechas Ramírez - **Delegatura para la Función Jurisdiccional y de** Conciliación

María Niny Echeverry Prada - **Delegatura para la Protección al Usuario**

María Yuleidy López Ramírez - **Delegatura para Entidades de Aseguramiento en Salud**

Edilma Marlen Suarez Castro - **Delegatura para Entidades Territoriales y Generadores, Recaudadores y administradores de Recursos del SGSSS**

Beatriz Eugenia Gómez Consuegra - **Delegatura para Prestadores de Servicios en Salud**

Mónica Patricia Almonacid Guzmán - **Delegatura para Operadores Logísticos de Tecnologías en Salud y Gestores Farmacéuticos**

Gloria Rocío Pereira Oviedo - **Jefe Oficina Asesora de Planeación**

Jazmín Maritza La Rotta Bernal - **Jefe Oficina Asesora de Comunicaciones Estratégicas e Imagen Institucional**

Gressy Kareny Rojas Cardona-**Dirección Jurídica**

Juan Sebastián Emanuel Sierra Álvarez - **Oficina de Liquidaciones**

José Alexander de los Reyes Aldana - **Dirección de Innovación y Desarrollo**

Giovanny López Mejia-**Oficina de Control Interno**

Contenido

Plan De Tratamiento de Riesgos de Seguridad y Privacidad De La Información

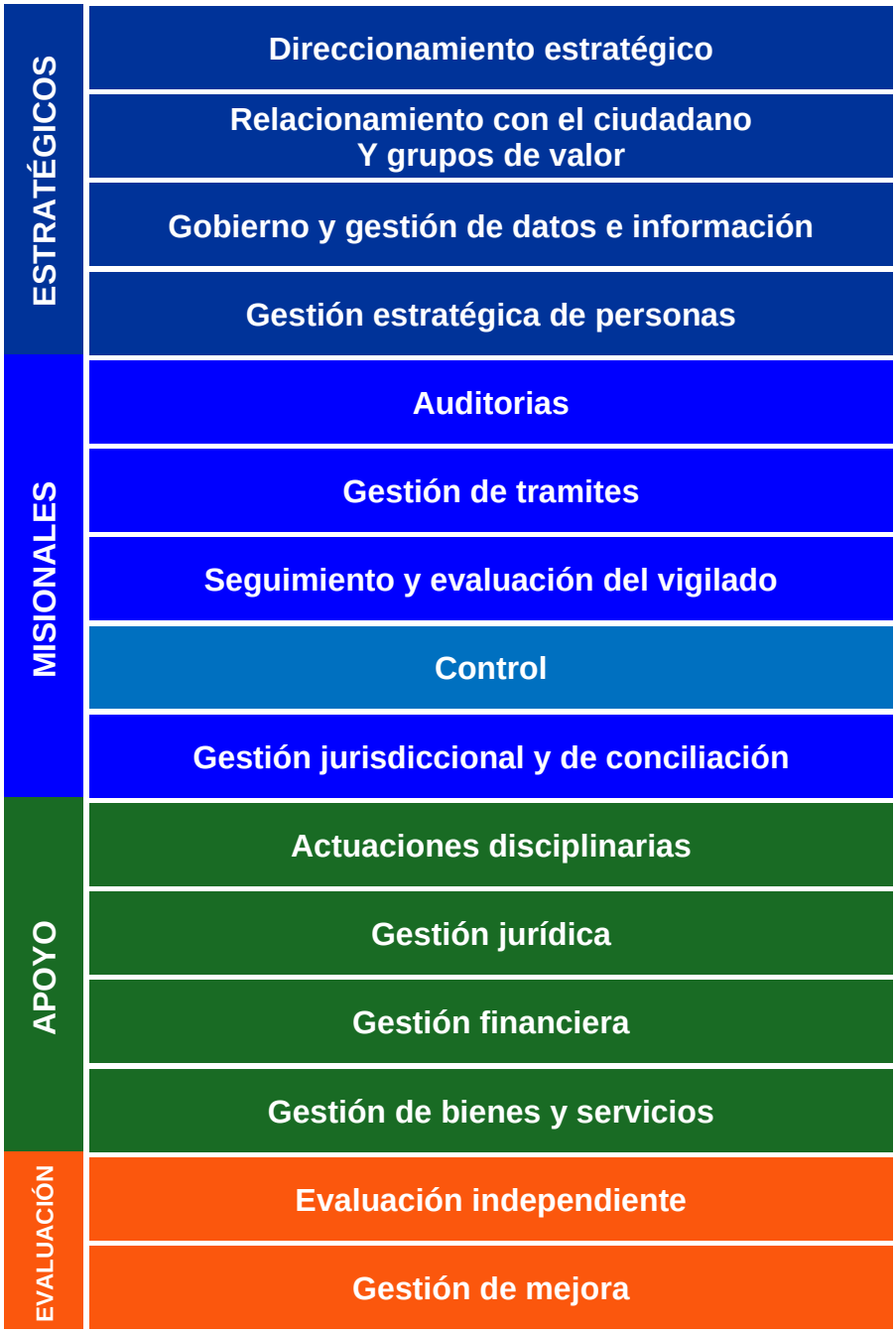
1. Propósito del plan

Alcance: Realizar una eficiente gestión de riesgos de seguridad digital a través del plan de tratamiento de riesgos, que permita ser integrado y aplicado a todos procesos, proyectos, servicios y planes de la entidad, se enfoca en gestionar y tratar todos los riesgos de seguridad de la información, con la finalidad de generar mecanismos de prevención y mitigación de los mismos, fortalecer la toma de decisiones y la prevención frente a la materialización de incidentes de seguridad de la información que puedan afectar el logro de los objetivos institucionales. Incluye directrices para gestionar de manera adecuada los riesgos de gestión.

- El Plan de Tratamiento de Riesgos contempla las etapas de:
- Identificación, análisis, tratamiento, monitoreo y seguimiento de los riesgos.
- Implementación de controles preventivos, detectivos y correctivos

Riesgos clasificados en nivel Moderado, Alto y Extremo, de acuerdo con la Guía de la Función Pública, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad. Se busca garantizar la protección de activos críticos y la prevención de incidentes que puedan afectar la misión institucional. Así mismo se orienta hacia la identificación y protección de nuestros activos críticos, así como hacia la implementación de controles necesarios para su mitigación, y crear una cultura organizacional adaptada en la importancia y la responsabilidad compartida en la protección de activos de seguridad de la información sensible de la Entidad.

Ilustración 1 Mapa de procesos de la Superintendencia Nacional de Salud que hacen parte del alcance del SGSI



Objetivos generales

Establecer y aplicar en la Superintendencia Nacional de Salud los lineamientos del Plan de Tratamiento de Riesgos de Seguridad Digital, para tratar de manera integral los riesgos de seguridad digital que faciliten la toma de decisiones y reduzcan la probabilidad e impacto de amenazas y vulnerabilidades sobre los activos de información, protegiendo y preservando la integridad, confidencialidad, y disponibilidad de la información, en apoyo al cumplimiento de los objetivos institucionales.

Objetivos Específicos

- Realizar monitoreo y seguimiento de acuerdo con la POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DEMN02, establecida en la Superintendencia Nacional de Salud; con el fin de verificar la efectividad de los controles de cada uno de los riesgos.
- Establecer actividades con los responsables de los procesos respecto a la seguridad de la Información, para la implementación del plan de tratamiento de riesgos.
- Identificar y actualizar los riesgos de seguridad de la información de la Entidad.
- Gestionar los riesgos de seguridad de la información, conforme al análisis, evaluación y valoración de estos, para preservar la integridad, disponibilidad y confidencialidad de los activos de información.
- Implementar y hacer seguimiento a los controles definidos para mitigar los riesgos de Alto y Extremo.
- Sensibilizar y capacitar a los responsables de procesos sobre la importancia de la seguridad de la información, y el adecuado tratamiento de los activos de información y sus riesgos.

- Realizar seguimiento periódico a los planes de tratamiento, verificando la efectividad de los controles.
- Promover la mejora continua mediante la definición de indicadores de gestión y lecciones aprendidas. para así proponer controles que apunten a minimizar la probabilidad de materialización de los riesgos identificados.

Definiciones

ACTIVO DE INFORMACIÓN. En el contexto de seguridad de la información, son elementos tales como aplicaciones de la entidad, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que tenga valor para la organización y que utiliza para funcionar en el entorno digital.

ADMINISTRACIÓN DEL RIESGO: Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

AMENAZA**:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

ANÁLISIS DEL RIESGO: Establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente) y posterior a la definición de controles para prevenir la ocurrencia del riesgo (análisis del riesgo residual).

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

CONFIDENCIALIDAD. Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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.

CONTROL. Medida que modifica al riesgo.

DESCRIPCIÓN DEL RIESGO: Narración o explicación de las siguientes preguntas: ¿Qué puede suceder?, ¿cómo puede suceder?, ¿cuándo puede suceder? y ¿qué consecuencias tendría su materialización?

DISPONIBILIDAD. Propiedad de que la información sea accesible y utilizable a demanda por la entidad.

EVALUACIÓN DEL RIESGO: resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo.

IDENTIFICACIÓN DEL RIESGO: etapa de administración del riesgo donde se definen los riesgos con sus causas, agentes generadores asociados a las causas, consecuencias, definición de productos y/o servicios que pueden afectarse con la materialización del riesgo, situaciones de deño antijurídico y clasificación.

INTEGRIDAD. Propiedad de exactitud y completitud de la información.

IMPACTO. Consecuencias que puede ocasionar a la organización la materialización del riesgo.

MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Permite tener una visión general de los riesgos de seguridad que pueden afectar los grupos de activos de los diferentes procesos de la entidad.

IVELES DE ACEPTACIÓN DEL RIESGO: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular

PROBABILIDAD. Posibilidad de ocurrencia de un riesgo. Está 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 período de 1 año.

REDUCCIÓN DEL RIESGO: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

RIESGO. Probabilidad de que una amenaza específica aproveche una vulnerabilidad, causando pérdida o daño a un activo de información. Esto generalmente se considera como una combinación de la probabilidad de que ocurra un evento y sus consecuencias.

RIESGO INHERENTE. Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

RIESGO RESIDUAL. El resultado de aplicar la efectividad de los controles al riesgo inherente busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos.

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).

SEGURIDAD DE LA INFORMACIÓN. Procesos, procedimientos, controles, guías y medidas preventivas y correctivas que las personas, entidades y las organizaciones adoptan para resguardar y proteger la información y los activos de información, buscando mantener la confidencialidad, disponibilidad e integridad de estos (ISO/IEC 27000).

VULNERABILIDAD. Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

2. Diagnóstico de la situación

La metodología para el tratamiento de los riesgos de seguridad y privacidad de la información derivados de los procesos y actividades de la entidad se encuentra integrada en la Política de Administración del Riesgos, mediante la definición e implementación del procedimiento de Administración del Riesgo, que para calificar el impacto de los riesgos, incluye los niveles de aceptación, tratamiento (mecanismos de prevención y mitigación), seguimiento y evaluación", la cual busca identificar, valorar, planificar y adelantar el tratamiento oportuno y mantener los riesgos en niveles óptimos de control para así preparar a la SNS ante una posible materialización y adelantar procesos de seguimiento, monitoreo, evaluación, o auditoría, según corresponda.

El proceso de identificación de riesgos de Seguridad de la información inicia con la ejecución de la matriz Identificación de Activos de Información DIFT46, a través de la cual se realiza la identificación, valoración y clasificación de los activos de información de cada uno de los procesos de la SNS y continua con el desarrollo de las siguientes actividades, las cuales permiten la identificación de los riesgos de seguridad de la información, su valoración y el establecimiento de los controles necesarios para su mitigación:

Establecimiento del contexto

Permite describir el entorno, así como las situaciones particulares de la Entidad para el análisis de los riesgos.

Identificación riesgos

Para cada tipo de activo o grupo de activos críticos pueden existir una serie de riesgos, los cuales la entidad debe identificar, valorar y posteriormente

Evaluación de riesgos

Se determinan los riesgos que por su impacto y probabilidad de ocurrencia pueden afectar el cumplimiento de las metas y objetivos de la dependencia.

Tratamiento de riesgo

Una vez se han identificado los riesgos, se define el tratamiento para cada uno de los riesgos analizados y evaluados, conforme a los criterios y al apetito de riesgo definidos (Evitar, aceptar, compartir o mitigar el riesgo).

Aceptación del riesgo

Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo

3. Estrategias

Los Riesgos de Seguridad de la Información son identificados, valorados y tratados de acuerdo con la POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DEMN02, establecida en la Superintendencia Nacional de Salud.

La Superintendencia Nacional de Salud ha iniciado, por primera vez, la gestión de los riesgos relacionados con la seguridad de la información en el marco de la implementación de su Modelo de Seguridad y Privacidad de la Información, alineando sus manuales y herramientas con los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la “Guía para la Administración del Riesgo, la Política de Administración de Riesgos de la Superintendencia Nacional de Salud DEMN02 y el diseño de controles en entidades públicas.

Esta gestión busca anticipar y mitigar posibles amenazas que puedan comprometer el cumplimiento de su misión y visión institucional, a través del impacto en la confidencialidad, integridad o disponibilidad de sus activos de información.

3.1. Tratamiento del riesgo

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

Ilustración 2 Estrategias para combatir el riesgo

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

3.2. Política Administración de Riesgos

La política de administración del riesgo es la declaración de la alta dirección para la gestión del riesgo donde permitirá desarrollar los lineamientos metodológicos aplicables del ciclo de administración de riesgos de seguridad y privacidad de la información de la Superintendencia Nacional de Salud, mediante la identificación,

análisis, evaluación, tratamiento de los riesgos con el fin de asegurar el cumplimiento de los objetivos de la entidad.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

METODOLOGÍA

El Plan de Tratamiento de Riesgos plantea, contempla la metodología y actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad se encuentra integrada en la política de Administración de riesgos tomando como referencia la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas versión 6, lo cual conduce no solo a una gestión pública más eficiente, sino también servirá para que se cumpla con los objetivos corporativos.

Los controles seleccionados para mitigar los riesgos de Seguridad digital serán confrontados con los estándares ISO/IEC 27001; a fin de determinar las falencias de la entidad en este sentido.

Desarrollo Metodológico

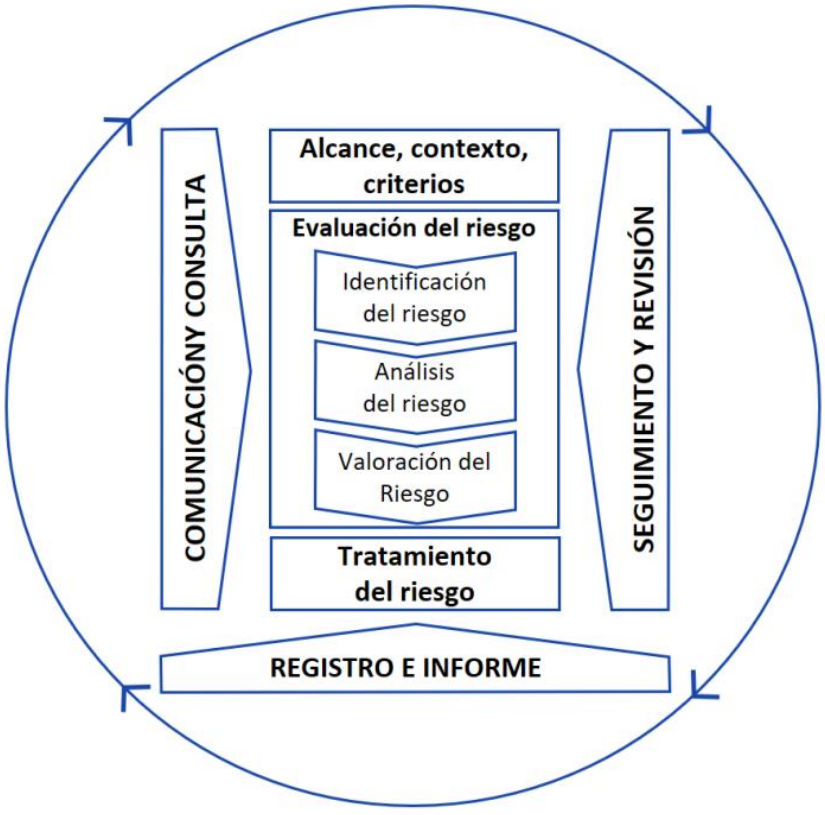
La metodología para la Administración del Riesgo requiere de un análisis inicial

relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, el

conocimiento de esta, desde un punto de vista estratégico de la aplicación de tres (3) pasos básicos para su desarrollo.

Contempla las etapas de Análisis del contexto, Evaluación del riesgo (Identificación, análisis y valoración), Tratamiento del riesgo, Registro e informe, Comunicación y consulta, y Seguimiento y revisión, como se muestra en el siguiente gráfico:

Ilustración 3 Proceso de gestión de riesgos, adaptado de la NTC-ISO 31000 Gestión del Riesgo-Directrices–2018.



Fuente: Proceso de gestión de riesgos, adaptado de la NTC-ISO 31000 Gestión del Riesgo-Directrices–2018

Análisis de la información:

Fase 1: En esta fase se revisan los resultados de las mesas de trabajo con los diferentes procesos de la Entidad para desarrollar las siguientes actividades:

• Verificar y analizar los riesgos identificados.

• Determinar los controles aplicables a cada riesgo.

• Definir los planes de tratamiento de los riesgos que superen al apetito aceptable.

Fase 2: Desarrollo de las medidas de tratamiento de riesgos en esta fase se realizarán las siguientes actividades:

• Determinar la medida de tratamiento.

• Definir los responsables de cada medida.

• Establecer el objetivo de cada medida.

• Desarrollar las acciones de cumplimiento de cada medida.

Fase 3: Análisis de los riesgos y medidas aplicadas

• Validar la eficacia de los controles, medidas de mitigación y tratamiento.

• Analizar la aplicabilidad de las medidas de mitigación y tratamiento.

Fase 4: Ciclo de vida del tratamiento de riesgos.

• Actividades del Plan de Tratamiento de Riesgos

Identificación/ Actualización del Riesgo:

Identificación de activos con Criticidad Alta: De acuerdo con el resultado de la matriz de activos de información cada uno de los procesos debe realizar la identificación de los activos cuya valoración de criticidad del activo sea alta, hacer

el análisis de los activos teniendo en cuenta la calificación en términos de confidencialidad, integridad y disponibilidad.

Para cada riesgo identificado se deben determinar las causas que lo originan (¿por qué sucede?); luego, los factores de riesgos (agentes generadores) asociados a cada una de estas y sus consecuencias.

En la identificación del riesgo se deben satisfacer las siguientes condiciones:

✓ Enfocarse en el objetivo y salidas del proceso.

✓ Describir el riesgo de forma clara y concisa.

✓ NO describir el riesgo como una negación.

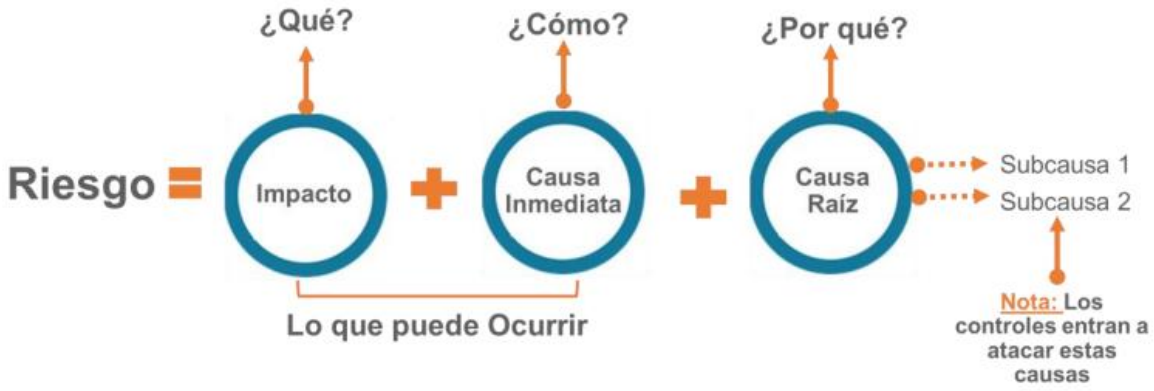
✓ NO describir el riesgo como una deficiencia o ausencia del control.

✓ NO iniciar la descripción del riesgo con expresiones como **Falta de, Deficiencias, Debilidades y otras similares**, dado que las mismas se relacionan con posibles causas del riesgo.

✓ Cada riesgo debe acotarse y precisarse. Un riesgo demasiado amplio o general conlleva que cualquier desviación en la operación de los procesos, relacionada con aquel, pueda interpretarse equivocadamente como materialización del riesgo.

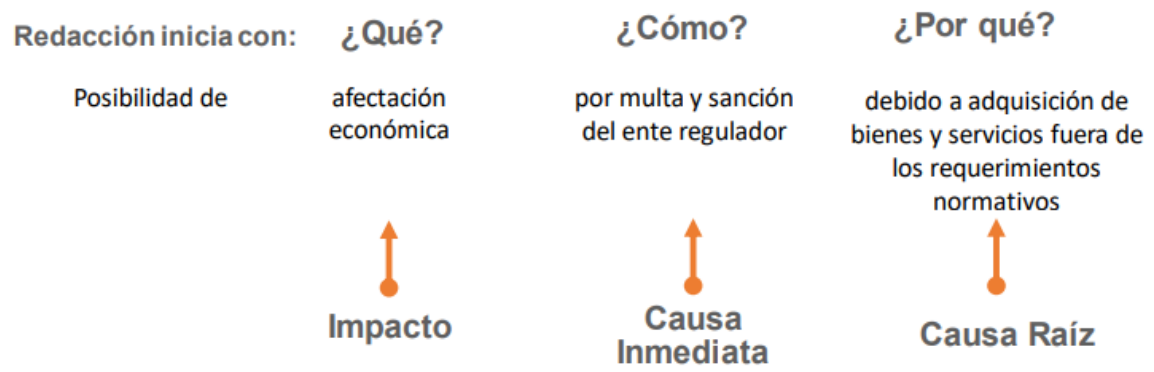
Únicamente se configura materialización de riesgos si existe evidencia objetiva de que la misma produce afectaciones económicas, reputacionales y/o de imagen a la entidad, dado que no toda desviación en la operación de los procesos corresponde, per se, a materialización de riesgos. Además, la inexistencia o falla en la aplicación de controles en los procesos no es materialización de riesgos.

Ilustración 4 Estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

Ilustración 5 Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

3.3. Valoración del Riesgo:

Se establecen los criterios para analizar probabilidad e impacto del riesgo identificado y su nivel de severidad, con enfoque en la exposición al riesgo, análisis que permite a los líderes de proceso contar con elementos objetivos para definir, se consideran la afectación económica y reputacional como aspectos

principales frente a la posible materialización de los riesgos, según la escala de severidad definida en (baja, moderada, alta y extrema), elementos que plantean un análisis de mayor profundidad según el entorno cambiante de la Entidad.

Tratamiento Zona de Riesgo Final:

• Zona de riesgo Baja: Aceptar el riesgo.

• Zona de riesgo Moderada: Reducir el riesgo.

• Zona de riesgo Alta: Reducir el riesgo, evitar, transferir o compartir.

• Zona de riesgo Extrema: Reducir el riesgo, evitar, transferir o compartir

Los riesgos que se encuentren en zona baja se aceptan (apetito del riesgo) y se continúa el monitoreo, con el fin de garantizar que las condiciones bajo las cuales han sido analizados no han cambiado, si las condiciones cambian, es necesario volver a valorar y si es el caso determinar el manejo correspondiente a través de los controles que sean necesarios

En esta etapa se realizan actividades tendientes a apoyar a los procesos a través de mesas de trabajo en la identificación de los riesgos de seguridad de la información sobre los activos valorados con criticidad ALTA, y se realizan las siguientes actividades:

4. Planes, proyectos y programas asociados

(En esta sección se debe relacionar los Planes, Proyectos y programas asociados el presente plan).

PROGRAMACIÓN Y AGENDAMIENTO DE MESAS DE TRABAJO:

Se realiza la programación de reuniones con los líderes de activos asignados por cada uno de los procesos.

ENTREVISTA CON LOS LÍDERES DE ACTIVOS: Se entrevista a cada líder asignado, se realiza la revisión de los activos cuya criticidad sea alta y se validan los criterios (confidencialidad, integridad y disponibilidad) cuya calificación haya sido alta, con el fin de identificar que riesgos podría afectar ese cada criterio valorado como alto.

IDENTIFICACIÓN Y CALIFICACIÓN DE RIESGOS INHERENTES: En esta fase es clave contar con información coherente y actualizada de las actividades que se llevan a cabo en los diferentes procesos, los resultados esperados de las mismas y orígenes de riesgos, identificando el nivel de riesgo inherente de acuerdo con la metodología establecida en el documento POLÍTICA DE ADMINISTRACIÓN DE RIESGOS DEMN02.

IDENTIFICACION DE CONTROLES: Con el fin de fortalecer el enfoque preventivo, correctivo y detectivo se determinan los controles actuales que permiten gestionar de manera efectiva los riesgos teniendo en cuenta y sin limitarse al anexo A. de la norma ISO 27001:2022, identificando el responsable, la frecuencia de ejecución del control, el propósito, procedimiento o la Acción como se aplica el control, la evidencia, y las observaciones en consonancia con los lineamientos institucionales.

VALORACIÓN DE CONTROLES: En esta etapa de acuerdo con los criterios establecidos en la metodología se hace una proyección de la eficacia de los controles para calcular el riesgo residual, esto permite determinar si el control responde de manera efectiva al tratamiento del riesgo.

CALIFICACION DEL RIESGO RESIDUAL: En esta fase se ubican los riesgos en el mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles y se determina el riesgo final que queda después de la aplicación de los controles, con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por el Ministerio. Si el riesgo se ubica en una zona No Aceptable (Altos y Extremos), cada líder de proceso es responsable de los riesgos identificados y con el apoyo del Oficial de Seguridad de la Información, define e implementan los controles que permitan disminuir el impacto y la probabilidad para llevar el riesgo a un nivel Aceptable.

5. Cronogramas

A continuación, se describen las actividades y las fechas de ejecución propuestas para la ejecución de las iniciativas.

Ver anexo. Cronograma Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026.

https://supersalud.sharepoint.com/:x:/r/sites/GrupodeSeguridadDigital/Documentos%20compartidos/MONITOREO%20DE%20RIESGOS%20DE%20SEGURIDAD/Cronograma%20Tratamiento%20Riesgos%202025.xlsx?d=w17cbbbe5973d4a48b1c0983d34002701&csf=1&web=1&e=nJ7ucE

6. Metas e indicadores asociados

Los Planes de Tratamiento de riesgos están intrínsicamente relacionados con los indicadores estratégicos y tácticos definidos en la SNS, por tanto, la medición se realizará a través de dichos indicadores.

El monitoreo de los riesgos de Seguridad Digital y Privacidad de la Información de la Superintendencia Nacional de Salud, aprobados por los procesos, así como de sus controles y planes de tratamiento, se realiza por parte del profesional asignado de cada proceso, así como el profesional de Seguridad y Privacidad de la Información con el apoyo de los profesionales de la Oficina Asesora de Planeación, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos a los procesos:

Seguridad y Privacidad de la información, Plan de Tratamiento de Riesgos de seguridad digital y privacidad de la información 2025 realizados, así como el cargue de los soportes correspondientes a los controles definidos.

Una vez los procesos realicen el reporte de cumplimiento de sus planes de tratamiento y controles, el profesional del proceso de Seguridad y Privacidad de la Información realiza la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través del indicador que tiene como propósito medir el nivel de implementación de los controles en los riesgos de Seguridad Digital de la Superintendencia Nacional de Salud. Se medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador:

Toda vez que el presente Plan está integrado al Plan de Acción Institucional de la vigencia, el seguimiento se realizará cuatrimestralmente y se reportará el resultado de cada período, en el instrumento de seguimiento al Plan de Acción, en el compromiso asociado al Plan de Seguridad y Privacidad de la Información.

Seguimiento

Se debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

• Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.

• Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

• Realizar monitoreo de los riesgos y controles tecnológicos.

• Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.

• Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.

• Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles

Responsable del seguimiento:

Líder – Subdirección de Tecnologías de la Información con apoyo del equipo de Seguridad digital.

7. Riesgos Asociados

OPORTUNIDAD DE MEJORA

El análisis de los riesgos debe ser la base para la identificación de nuevas oportunidades de mejora en cada uno de los procesos de la entidad, lo cual es una consecuencia positiva producto del resultado del tratamiento del riesgo.

ACTIVIDADES

Las actividades se desarrollan de acuerdo con lo establecido en el mapa de riesgos de la Superintendencia Nacional de Salud, donde están relacionadas cada una de las acciones a desarrollar por cada proceso que se relacionarán en la matriz del mapa de riesgos Institucional publicada en el sitio web de la entidad, página procesos, pestaña Mapa de riesgos institucional: https://www.supersalud.gov.co/es-co/nuestra-entidad/estructura-organica-y-talento-humano/procesos

8. Fuentes de financiación

Este plan se lleva a cabo con recursos propios: humanos, físicos, tecnológicos y financieros; con énfasis en aplicación de controles y acciones para gestionar los riesgos, el seguimiento y control de la gestión, así como la implementación de las acciones de control definidas en este plan están bajo la responsabilidad del dueño del riesgo.