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

2024

Bogotá, enero 2024

CONTENIDO

Página

OBJETIVO....3
ALCANCE....3
ABREVIATURAS O SÍMBOLOS....3
DEFINICIONES....3
MARCO NORMATIVO....5
POLITICAS O LINEAMIENTOS GENERALES....5
CONDICIONES DE SEGURIDAD....5
DESCRIPCIÓN DE ACTIVIDADES O CONTENIDO PRINCIPAL....5
DOCUMENTOS RELACIONADOS....8
REFERENCIAS BIBLIOGRÁFICAS....8
ANEXOS....8

OBJETIVO

Hacer seguimiento al plan de tratamiento de riesgos de seguridad y privacidad de la información del INM el cual se alinea con la estrategia de gobierno digital de Ministerio TIC, a través de la implementación del modelo de gestión de riesgo de seguridad de la información de entidades públicas, DAFP para lograr la mitigación o reducción de materialización de riesgos de seguridad que puedan afectar la confidencialidad, integridad y disponibilidad de la información del INM.

ALCANCE

El seguimiento a los planes de tratamiento actuales se llevará acabo basado en la matriz de riegos de seguridad de la información existente.

La gestión de riesgos de seguridad de la información se lleva a cabo con base en el matriz de activos de información del INM, En su proceso de madurez y mejoramiento, se actualizará si se evidencian riesgos de seguridad adicionales a los existentes en las diferentes áreas.

ABREVIATURAS O SÍMBOLOS

INM: Instituto Nacional de Metrología

MinTic: Ministerio de las telecomunicaciones

DAFP: Departamento administrativo de la Función Pública

POSI: Plan de seguridad y privacidad de la información

DEFINICIONES

- **Activos**

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).

- **Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **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).

- **Riesgo**

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**

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Vulnerabilidad**

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

MARCO NORMATIVO

- Modelo de gestión de riesgo de seguridad de la información de entidades públicas, DAFP.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6.
- ISO 27001:2022.

POLITICAS O LINEAMIENTOS GENERALES

- El plan será liderado por el responsable de seguridad de la información. Sin embargo, para el éxito de la implementación de éste es necesaria la participación de personal de los diferentes procesos involucrados.
- El plan de tratamiento de riesgos debe ser establecido e implementado por el responsable del riesgo.
- El INM debe proporcionar los recursos necesarios para el tratamiento de los riesgos, para así poder llevar a cabo eficazmente su implementación.

CONDICIONES DE SEGURIDAD

El plan de riesgos de seguridad de la información debe ser tratado como un documento confidencial.

DESCRIPCIÓN DE ACTIVIDADES O CONTENIDO PRINCIPAL

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información son las acciones que se establecen para reducir los riesgos de Seguridad Digital que superan el nivel de riesgo aceptable de la organización. Este resultado se obtiene de la evaluación de la probabilidad de ocurrencia por el impacto que ocasionaron o podrían ocasionar las amenazas por el aprovechamiento de las vulnerabilidades de los activos de seguridad digital de la organización.

La implementación del Modelo de Seguridad y Privacidad de la información, toma como base los lineamientos planteados en el estándar de seguridad ISO27001:2022, así como los principios regulatorios de gobierno en línea. Estos lineamientos apoyan su enfoque en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información.

Para ese tratamiento de riesgos, el Gobierno Nacional ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción

y de seguridad de la información y para el enfoque particular de los riesgos de seguridad de la información ha establecido el Modelo de gestión de riesgo de seguridad de la información de entidades públicas, DAFP.

En INM se ha venido trabajando la estructuración de los riesgos de seguridad de la información, basados en dicho modelo de gestión de riesgo, DAFP.

La gestión de riesgos dentro de su fase de valoración de riesgos incluye el monitoreo y revisión de riesgos, como se observa en el gráfico de Metodología para la administración de riesgos. Esta actividad se hará periódicamente para poder hacer un tratamiento de riesgos óptimo y eficaz.

Basados en esta premisa, el plan de tratamiento de riesgos de 2024 en INM, se enfocará en los siguientes actividades:

a. Identificar los riesgos inherentes de seguridad de la información

Como lo indica la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. para efectos del presente modelo se identifican los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para la determinación de amenazas y vulnerabilidades se toma como base las sugeridas por el Modelo Nacional de riesgos de seguridad y las amenazas conocidas que se han materializado a nivel nacional y mundial.

Esta identificación de riesgos se desarrolló durante el 2023. En el 2024 solamente se identificarán riesgos, que se detecten de situaciones particulares y que no estén ya contemplados en la matriz de riesgos de seguridad de la información.

b. Valoración Del riesgo

Para esta etapa se asocian las tablas de probabilidad e impacto definidas en el INM, en el proceso de gestión de riesgos liderado por el área de planeación, las cuales se basan en Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información.

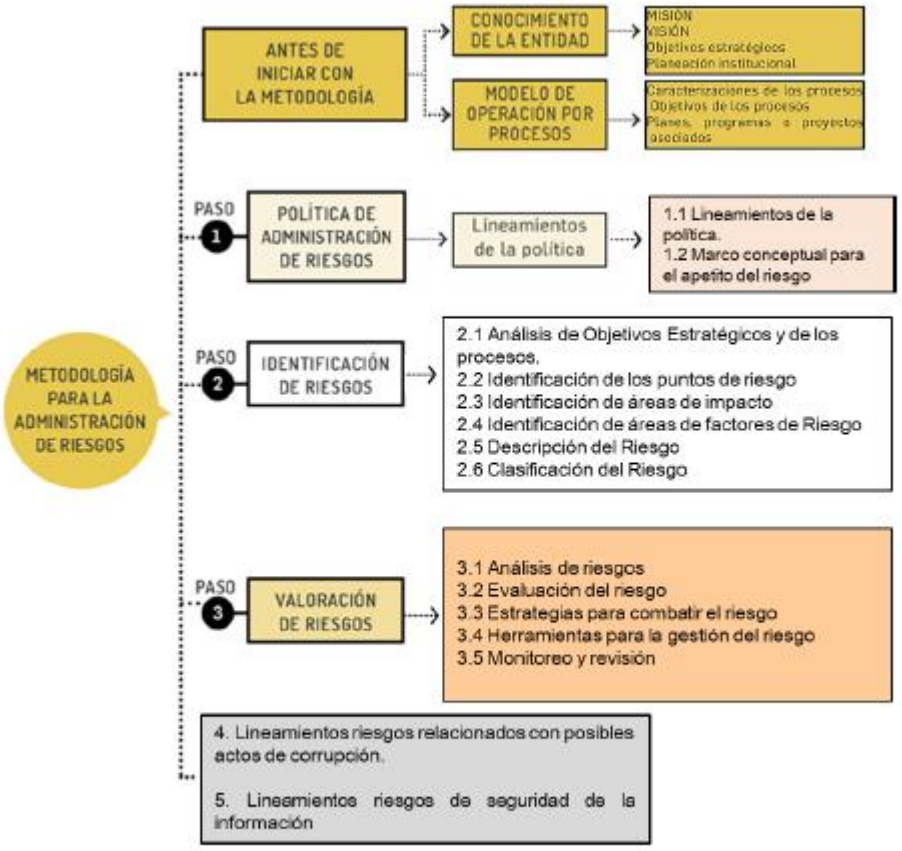
c. Controles asociados a la seguridad de la información

Para mitigar/tratar los riesgos de seguridad de la información se emplean los controles del Anexo A de la ISO/IEC 27001:2022.

d. Tratamiento de los riesgos de seguridad de la información

Se hará seguimiento cuatrimestral a los planes de tratamiento de riesgos establecidos. Esta actividad se hace en conjunto con las áreas involucradas.

Posteriormente se harán actividades de monitoreo y revisión, validación de los riesgos residuales, y efectividad de los planes de tratamiento o los controles implementados. Esto se alinea con la fase de evaluación y desempeño descrita en el plan de seguridad y privacidad de seguridad de la información.



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

e. Riesgos de seguridad de la información en Isolucion

En miras de la automatización y aprovechamiento de herramientas existentes, se trabajará en el cargue de los riesgos de seguridad de la información en el módulo de ISolucion,

dispuesto para esto y que permitirá facilitar la tarea de seguimiento de riesgos y planes de tratamiento posteriormente.

El plan de tratamiento de riesgos detallado se encuentra en el Anexo SEGUIMIENTO AL PLAN de Seguridad y Privacidad de la Información - VIGENCIA 2024 de la OIDT.

DOCUMENTOS RELACIONADOS

SEGUIMIENTO AL PLAN de Seguridad y Privacidad de la Información - VIGENCIA 2024

REFERENCIAS BIBLIOGRÁFICAS

1. Modelo de gestión de riesgo de seguridad de la información de entidades públicas, DAFP.
2. Modelo de Seguridad y Privacidad de la Información. MinTIC.
3. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas

Versión 6

ANEXOS

Anexo SEGUIMIENTO AL PLAN de Seguridad y Privacidad de la Información - VIGENCIA 2024.

Cronograma de actividades

ACTIVIDAD	PRODUCTO / ENTREGABLE	PROGRAMACIÓN											
		M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Informe de seguimiento a la matriz de riesgos de seguridad de la información	Informe de seguimiento a la matriz de riesgo												
Piezas comunicativas enviadas por intranet	Capturas de pantalla de las piezas	1											
Informe de ejecución de la actividad	Informe												
Manual actualizado	Manual												