Plan de tratamiento de riesgos de seguridad y privacidad de la información 2025

OIDT

Bogotá

Fecha (2024-12-26)

CONTENIDO

Página.

1. INTRODUCCIÓN

En este informe se presentará el plan de tratamiento de riesgos de seguridad y privacidad de la información del INM a llevar a cabo en el 2025, de tal forma que se establezcan los controles necesarios para mitigar, reducir o evitar la materialización de una amenaza que afecte la disponibilidad, confidencialidad o integridad de la información del INM.

2. ALCANCE

La gestión de riesgos de seguridad de la información se lleva a cabo siguiendo los lineamientos del procedimiento establecido en el INM E-02-P-009 GESTIÓN DE LOS RIESGOS. ANEXO 2. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, el cual fue actualizado en el 2024, basándose en los marcos normativos descritos en el siguiente capítulo.

3. 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.

4. 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.

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 y ha generado un procedimiento para la gestión de riesgos de seguridad de la información, sobre la cual se basará la gestión de riesgos de 2025: E-02-P-009 GESTIÓN DE LOS RIESGOS y su ANEXO 2. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos dentro de su fase de valoración de riesgos incluye el monitoreo y revisión de riesgos. Esta actividad se hará trimestralmente para poder hacer un tratamiento de riesgos óptimo y eficaz.

Basados en esta premisa, el plan de tratamiento de riesgos de 2025 en INM, se enfocará en las 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.

e. Riesgos de seguridad de la información en Isolucion

Como en 2024 se hizo el cargue de los riegos de seguridad de la información, en el 2025, se llevarán a cabo las acciones para iniciar la gestión de seguimiento y de los riegos en isolucion.

El plan de ruta de tratamiento de riesgos detallado se encuentra en Planes institucionales 2025 OIDT - Riesgos Seguridad y Privacidad

5. DOCUMENTOS RELACIONADOS

Planes institucionales 2025 OIDT - Riesgos Seguridad y Privacidad

6. 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

7. ANEXOS

N/A

Elaboró: Liliana Pineda Aponte
Responsable seguridad de la información
Fecha: 26/12/2024