Plan de Tratamiento de Riesgos de Seguridad de la Información

Oficina de Informática y Desarrollo Tecnológico

Bogotá

2023-04-04

Instituto Nacional de Metrología de Colombia - INM
Av. Cra 50 No 26-55 Int. 2 CAN - Bogotá, D.C. Colombia
Conmutador: (57 601) 254 22 22 - **Website**: www.inm.gov.co
E-mail: contacto@inm.gov.co - **Twitter**: @inmcolombia
Código Postal 111321.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

CONTENIDO

Página.

1. INTRODUCCIÓN

Hacer seguimiento y optimizar el plan de tratamiento de riesgos de seguridad y privacidad de la información del INM con el fin de alinearse 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 y así lograr la mitigación o reducción de riesgos de seguridad que puedan afectar la confidencialidad, integridad y disponibilidad de la información del INM.

2. ALCANCE

El seguimiento a los planes de tratamiento actuales se llevará acabo basado en la matriz de riegos de seguridad de la información existente y la optimización de la gestión de riesgos se llevará a cabo basada en los lineamientos del Modelo de gestión de riesgo de seguridad de la información de entidades públicas, DAFP.

La gestión de riesgos de seguridad de la información se hará con base en el matriz de activos establecida en el plan de seguridad y privacidad. Posteriormente se establecerán amenazas y vulnerabilidades relacionadas con dichos activos. Con base en esta información se hace la definición del riesgo, su valoración y evaluación de controles.

Una vez evaluados los riesgos se procede a establecer el plan de tratamiento de riesgos, al cual se le hará seguimiento periódicamente.

3. DESCRIPCIÓN METODOLÓGICA

El presente documento se estructura de conformidad a la metodología establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, capítulo 5 Lineamientos riesgos de seguridad de la información, 5.1. Identificación de los activos de seguridad de la información, 5.2. Identificación del riesgo, 5.3. Valoración del riesgo, 5.4 Controles asociados a la seguridad de la información del Departamento Administrativo de la Función Pública, versión 5, diciembre 2020.

3.1. 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.

3.2. DEFINICIONES

Activos: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (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).

3.3. 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.

3.4. CONDICIONES DE SEGURIDAD

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

4. PLAN DE TRATAMIENTO DE RIESGOS

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 debe hacer periódicamente para poder hacer un tratamiento de riesgos óptimo y eficaz.

Basados en esta premisa, el plan de tratamiento de riesgos de 2023 en INM, se enfocará en los siguientes actividades:

4.1. IMPLEMENTACIÓN DE PLANES DE TRATAMIENTO

Se llevarán a cabo las actividades definidas previamente para cada uno de los planes de tratamiento existentes actualmente en la matriz de riegos de seguridad de la información, de tal manera que les dé un cierre eficaz.

Los planes de tratamiento para los riesgos definidos en la matriz de riesgos de seguridad de la información son:

No. Riesgo	Descripción del riesgo	Plan de tratamiento
E03-R4	Posibilidad de pérdida reputacional por quejas de grupos de valor debido a pérdida de integridad de la información cuando personal no autorizado realiza publicaciones en las redes o modifica contenido.	Establecer políticas de gestión de acceso, divulgarlas a la entidad
E03-R4	Posibilidad de pérdida reputacional por quejas de grupos de valor debido a pérdida de integridad de la información cuando personal no autorizado realiza publicaciones en las redes o modifica contenido.	Validar implementación de políticas de gestión de accesos en la publicación de información en redes sociales
M03-R10	Posibilidad de pérdida de información por ataques o fallas de los sistemas informáticos debido a falta de generación de copias de respaldo de manera efectiva.	Establecer políticas de backups acorde a la criticidad de la información
		Asistencia a las capacitaciones programadas por el grupo de la OIDT en cuanto a seguridad de la información.
A06-R1	Posibilidad de afectación reputacional y económica por pérdida de Expedientes o piezas procesales debido a una inadecuada custodia y manejo de los documentos y carpetas que hacen parte de los expedientes.	Seguimiento a la aprobación de la TRD del proceso de control disciplinario
A06-R1	Posibilidad de afectación reputacional y económica por pérdida de Expedientes o piezas procesales debido a una inadecuada custodia y manejo de los documentos y carpetas que hacen parte de los expedientes.	Generar lineamientos de seguridad e implementar actividades para salvaguardar los documentos críticos de los procesos en un repositorio seguro y restringido
E05-R04	Pérdida de disponibilidad de la información contenida en los servidores de la entidad debido a la ausencia de políticas de uso aceptable pueden facilitar un espionaje remoto (ataque informático).	Establecer procedimientos de gestión de la operación de TI
		Establecer políticas de seguridad para gestión de la operación de TI

El planteamiento de estas actividades se basa en los controles planteados por la norma de seguridad ISO27001:2022 y se encuentran dentro del plan de seguridad y privacidad de la información 2023. El detalle de las actividades se desglosa en el cronograma propuesto en el siguiente capítulo.

Las actividades serán lideradas por el responsable de seguridad de la información, pero es de vital importancia la participación del personal responsable del riesgo, en cada una de las áreas.

4.2. ACTUALIZACIÓN DE MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Paralelamente también se llevará a cabo la actividad de actualización de la matriz actual de riesgos de seguridad de la información, garantizado que esté alineada con el Modelo de gestión de riesgo de seguridad de la información de entidades públicas y donde se identifique nuevos riesgos.

Para el cumplimiento de esta actividad y basados en los lineamientos de la guía “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Del DAFP, se llevarán a cabo las siguientes fases, para su desarrollo:

a. Identificación de los activos de seguridad de la información

Para llevar a cabo la identificación es necesario tener claramente identificados los activos de la organización. Esta actividad está planeada dentro del POSI.

b. 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 cada riesgo, se asociará el grupo de activos o activos específicos del proceso, y conjuntamente se analizarán las posibles amenazas y vulnerabilidades que podrían causar su materialización.

Esta identificación de riesgos, ser hará a través de entrevistas al personal y revisión de la documentación existente, como son: manuales, procedimientos, incidentes de seguridad o de disponibilidad ocurridos anteriormente.

Para la determinación de amenazas y vulnerabilidades se tomará 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.

c. Valoración Del riesgo

Para esta etapa se asociarán 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.

d. Controles asociados a la seguridad de la información

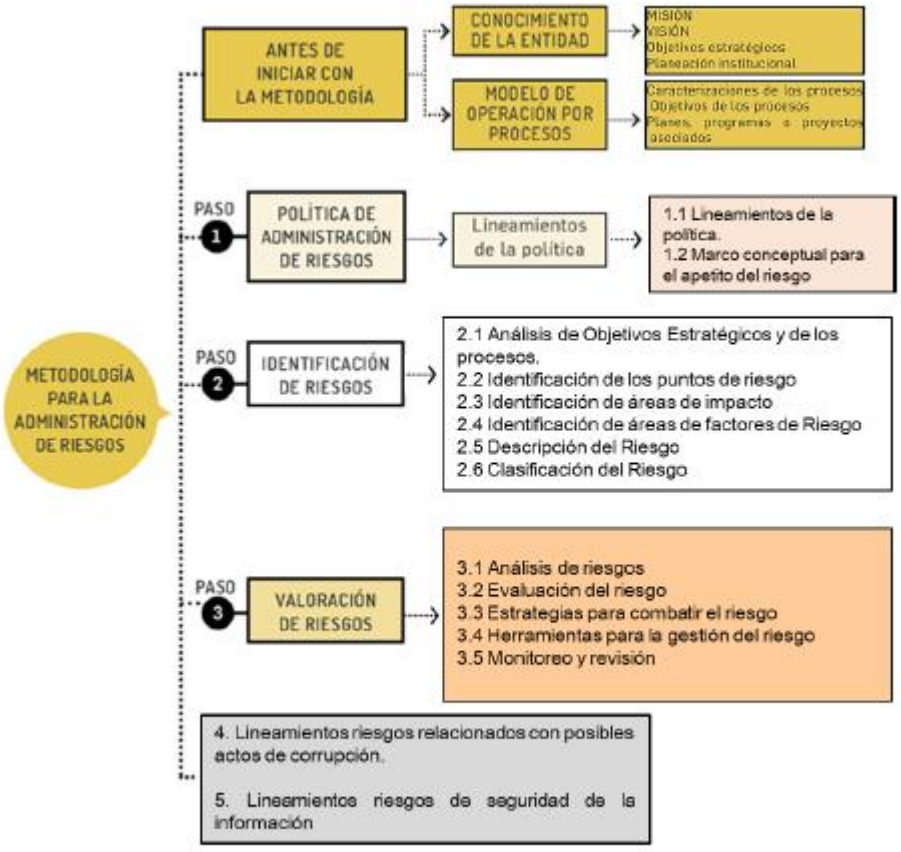
Para mitigar/tratar los riesgos de seguridad de la información se emplearán los controles del Anexo A de la ISO/IEC 27001:2022.

e. Tratamiento de los riesgos de seguridad de la información

Se establecerán las acciones para reducir o tratar los riesgos de Seguridad Digital que superan el nivel de riesgo aceptable de la organización. Y se hará seguimiento periódico a su implementación. Estas acciones se definen en conjunto con las áreas involucradas.

Adicionalmente se establecerán indicadores para medir la eficacia de cada uno de los planes.

Finalmente 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.

f. 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 2023 de la OIDT.

El detalle de las actividades se ve reflejado en el cronograma, presentado en el siguiente numeral.

4.3. CRONOGRAMA 2023

No. ÍTEM	No. RIESGO	DESCRIPCIÓN DEL RIESGO	ACTIVIDAD	PRODUCTO / ENTREGABLE	PROGRAMACIÓN												META ANUAL	RESPONSABLE
					M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12		
1	E03-R4	Posibilidad de pérdida reputacional por quejas de grupos de valor debido a pérdida de integridad de la información cuando personal no autorizado realiza publicaciones en las redes o modifica contenido.	Establecer políticas de gestión de acceso, divulgarlas a la entidad	Manual de políticas de seguridad actualizado y políticas socializadas					2								2	Responsable seguridad de la información- áreas involucradas
2	E03-R4	Posibilidad de pérdida reputacional por quejas de grupos de valor debido a pérdida de integridad de la información cuando personal no autorizado realiza publicaciones en las redes o modifica contenido.	Validar implementación de políticas de gestión de accesos en la publicación de información en redes sociales	Acta de validación de aplicación de políticas					1								1	Responsable seguridad de la información- áreas involucradas
3	M03-R10	Posibilidad de pérdida de información por ataques o fallas de los sistemas informáticos debido a falta de generación de copias de respaldo de manera efectiva.	Establecer políticas de backups acorde a la criticidad de la información	Documento de políticas de backups actualizado									1				1	OIDT
			Asistencia a las capacitaciones programadas por el grupo de la OIDT en cuanto a seguridad de la información	Listado asistencia a capacitación						1							1	Responsable seguridad de la información- áreas involucradas
4	A06-R1	Posibilidad de afectación reputacional y económica por pérdida de Expedientes o piezas procesales debido a una inadecuada custodia y manejo	Seguimiento a la aprobación de la TRD del proceso de control disciplinario	Matriz de riesgos actualizada con el seguimiento					1								1	Responsable seguridad de la información

		de los documentos y carpetas que hacen parte de los expedientes.																
5	A06-R1	Posibilidad de afectación reputacional y económica por pérdida de Expedientes o piezas procesales debido a una inadecuada custodia y manejo de los documentos y carpetas que hacen parte de los expedientes.	Generar lineamientos de seguridad e implementar actividades para salvaguardar los documentos críticos de los procesos en un repositorio seguro y restringido	Manual de políticas de seguridad actualizado y procedimiento de gestión de información crítica					1	1							2	Responsable seguridad de la información - OIDT- Área responsable
6	E05-R04	Pérdida de disponibilidad de la información contenida en los servidores de la entidad debido a la ausencia de políticas de uso aceptable pueden facilitar un espionaje remoto (ataque informático).	Establecer procedimientos de gestión de la operación de TI	Documento de procedimientos de la gestión de TI						1	1	1	1				4	Responsable seguridad de la información
			Establecer políticas de seguridad para gestión de la operación de TI	Manual de políticas de seguridad actualizado									1				1	Responsable seguridad de la información
7	N/A	N/A	Actualización de la matriz de riesgos de seguridad de la información, basado en los lineamientos de la guía del DAFP y la ISO27001: 2022	Matriz de riesgos actualizada								1					1	Responsable seguridad de la información
8	N/A	N/A	Cargar riesgos de seguridad de la información en isolucion.	Cantidad de riesgos cargados en isolucion					1					1			2	Responsable seguridad de la información

9	N/A	N/A	Seguimiento a los planes de tratamiento de seguridad de la información	Matriz de riesgos actualizada con el seguimiento					1			1			1	3	Responsable seguridad de la información
Revisó: **Oficina Asesora de Planeación**					**Aprobó:** **Comité Institucional de Gestión y Desempeño CIGD No. 5 del 2023-03-29 y 2023-04-04**													

5. ANEXOS

Cronograma Plan de Tratamiento de Riesgos de la Información.

LILIANA PINEDA APONTE

Contratista Seguridad de la Información

Fecha: 2023-04-04