

Informe de Evaluación y Seguimiento al Mapa de Riesgos y sus controles (Diseño y efectividad)

Oficina de Control Interno
Bogotá

2024-06-02

CONTENIDO

	Página.
1. INTRODUCCIÓN	3
2. ALCANCE	3
3. DESCRIPCIÓN METODOLÓGICA.....	3
4. RESULTADOS.....	6
5. CONCLUSIONES.....	32
6. RECOMENDACIONES.....	32
7. ANEXOS	33

1. INTRODUCCIÓN

En cumplimiento de las actividades definidas en el plan anual de auditoria para la vigencia 2024 en este caso el numeral 3. Rol de evaluación y gestión del riesgo se adelanta la presente evaluación y seguimiento al mapa de riesgos del Instituto y a las acciones de control propuestas desde los diferentes procesos para mitigar los riesgos identificados. Como insumo principal para ese análisis se tuvieron en cuenta los lineamientos definidos en la guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 de noviembre de 2022 emitida por la Función Pública.

A continuación, se citan entre otros los lineamientos normativos y criterios de carácter interno y externo que se consideraron para la elaboración del informe:

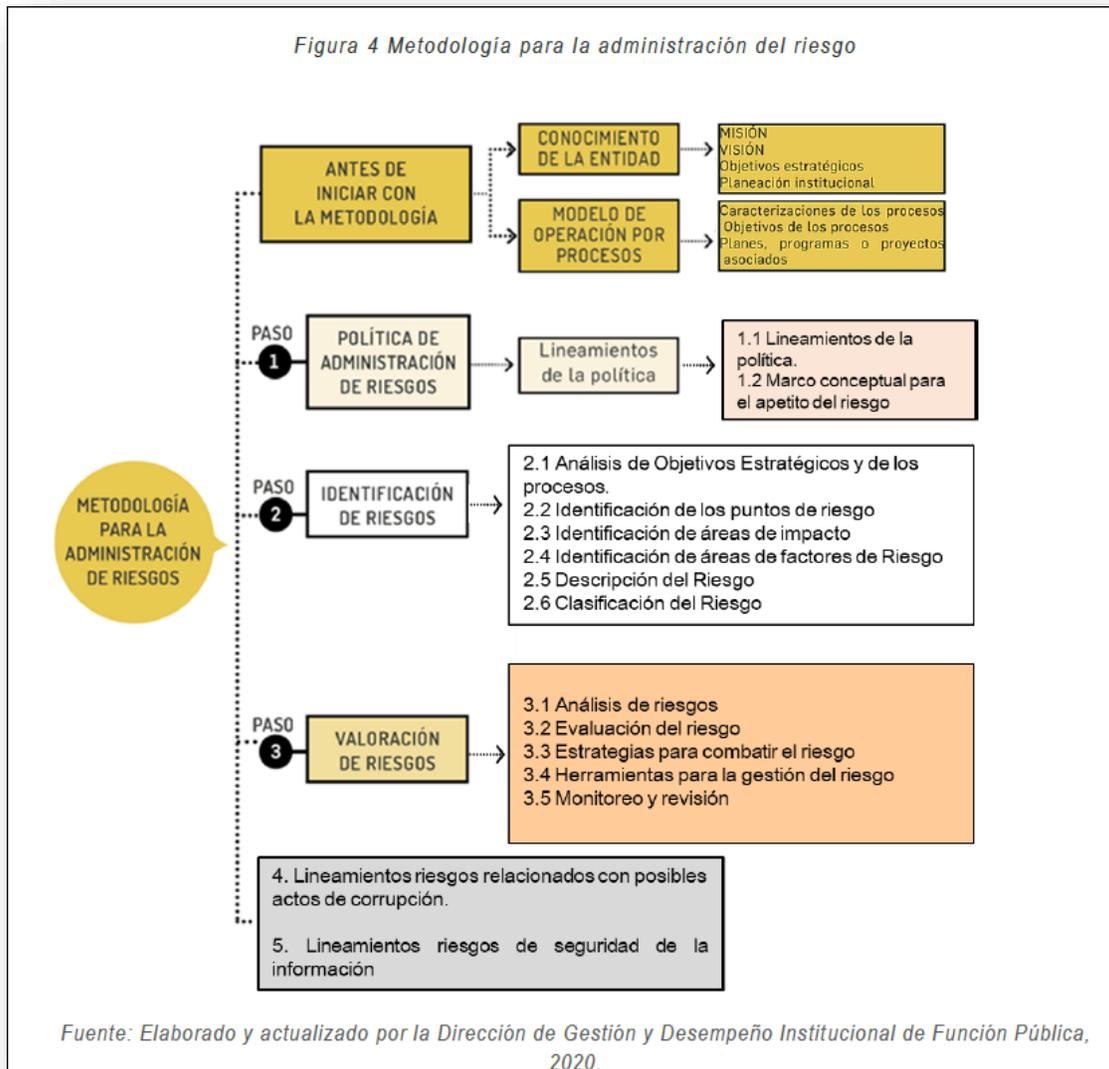
- ✚ Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."
- ✚ Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."
- ✚ Decreto 1081 de 2015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."
- ✚ Decreto 1083 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública". Artículo 2.2.23.2 "Actualización del modelo estándar de Control Interno".
- ✚ Manual Operativo del Modelo Integrado de Planeación y Gestión-MIPG, versión 5, marzo 2023, Consejo para la Gestión y Desempeño Institucional.
- ✚ Documento gestión del riesgo código E-02-D-001, versión 4 del 25 de abril de 2023 del Sistema de Gestión para consulta en el aplicativo Isolucion.

2. ALCANCE

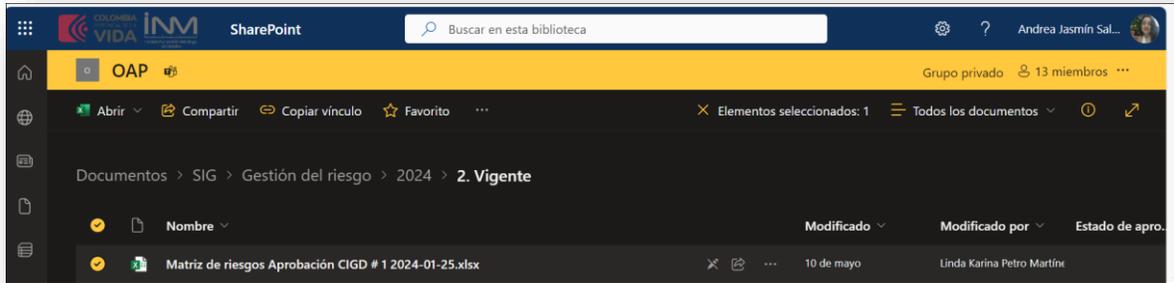
El presente informe comprende la verificación del mapa de riesgos aprobado en el Comité Institucional de Gestión y Desempeño No. 1 que se llevó a cabo en enero de 2024 en tres sesiones, el 25, 30 y 31 siendo esta última en la cual se aprobó el mapa.

3. DESCRIPCIÓN METODOLÓGICA

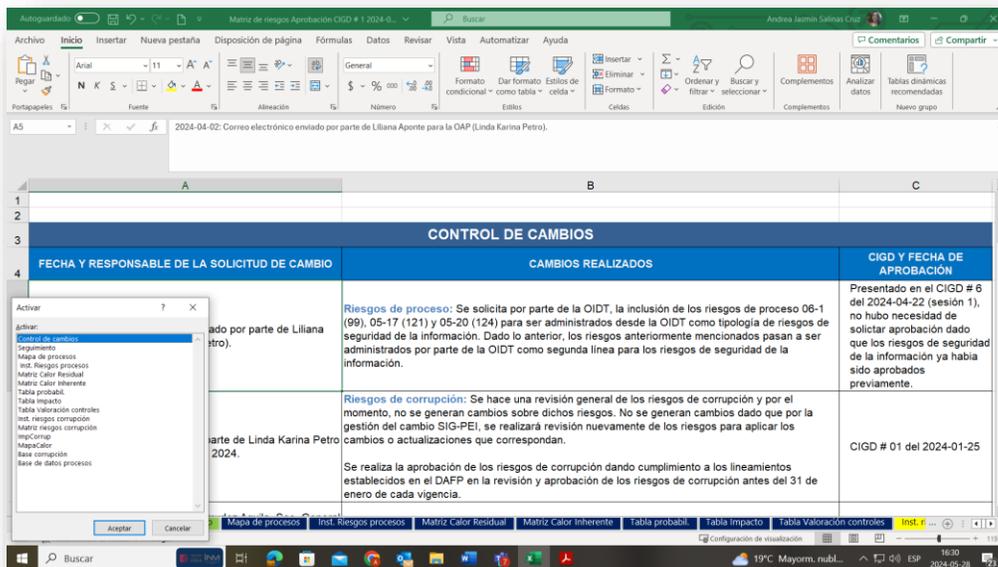
Para efectos de adelantar el presente informe se tuvo en cuenta la metodología dispuesta en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6 de noviembre de 2022 como se muestra en la siguiente imagen:



El otro insumo y el más importante para el presente análisis corresponde a la matriz de riesgos compartida por la Oficina Asesora de Planeación a través de correo electrónico en la ruta (OAP - Gestión del riesgo - Todos los documentos (sharepoint.com)) como se muestra a continuación:



El archivo en excel cuenta con 15 hojas (control de cambios, seguimiento, Mapa de procesos, ins. Riesgos procesos, matriz calor residual, matriz calor inherente, tabla probabilidad, tabla impacto, tabla valoración controles, inst. Riesgos corrupción, matriz riesgos corrupción, impCorrup, mapaCalor, base corrupción y base de datos procesos).



En cuanto a la fecha de aprobación de la matriz indicada en el mismo archivo es importante resaltar que la aprobación se realizó en la sesión 3 del CIGD #1 el 31 de enero de 2024 como quedó consignado en el acta y no en la sesión 1 que se llevó a cabo el 25 de enero de 2024.

Por otra parte, al realizar la consulta de los riesgos en Isolución en la pestaña riesgos DAFP se encontraron 130 como se puede visualizar en la siguiente imagen:

Sigla	Consecutivo	Versión	Fecha del Riesgo	Proceso	Objetivo del Proceso	Descripción del Riesgo	Alcance	Impacto	Causa Inmediata	Causa Raíz	Clasificación del Riesgo	Posibilidad de Ocurrencia	Impacto	Zona	Medidas de Respuesta	Desc.
[Empty rows representing the data in the matrix]																

4. RESULTADOS

A continuación, se muestran los resultados como parte del seguimiento efectuado:

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Según la guía para la administración del riesgo, la política de administración del riesgo se define como: <<La declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo...>>. Además, señala que la alta dirección, con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno, es la encargada de establecerla.

Por consiguiente, durante la sesión tres (3) del comité conjunto No. 1 CIGD y CICC, celebrada el 31 de enero de 2024, se refrendó y APROBÓ la política de administración del riesgo, según consta en el acta adjunta en la siguiente imagen:

13.2. Aprobación Matriz Riesgos Corrupción INM y política de riesgos

Linda Karina Petro, Profesional OAP, presentó para refrendación del CIGD, la política de la administración de los riesgos junto con la matriz de riesgos de corrupción. Laura Rivera, jefe OAP, mencionó que esta refrendación se hace en marco de las actividades del Programa de Transparencia y Ética Pública, por lineamientos normativos.

Comentarios: La directora general, comenta la importancia de darle una mayor relevancia al oficial de transparencia del INM y su labor. En el sentido de socializar y comunicar, quien es la persona designada y la forma en la que se puede relacionar y que se hace en la red interinstitucional de transparencia y corrupción.

Compromisos: Ninguno.

Conclusión: Los miembros del CIGD se dan por enterados y aprueban la Política de la Administración de los Riesgos y la Matriz Riesgos Corrupción del INM.

En cuanto a la publicación y divulgación en el numeral 8.1.1 del Manual Integrado de Gestión E-02-M-001, versión 9 del 6 de septiembre de 2023 cargado en Isolucion se menciona la política aprobada en el CICCI el 2023-03-13

Proceso	Código	Título Documento	Tipo de documento	Version	Usuario que revisa	Usuario que aprueba	Fecha Aprobacion
Administración del SIG	E-02-M-001	MANUAL INTEGRADO DE GESTIÓN	Manual	9	Laura Lorena Rivera Roa	Comité Institucional de Gestión y Desempeño	2023-03-13

8.1.1. Política de administración de riesgos
<p>El Instituto Nacional de Metrología de Colombia (INM) está comprometido con la gestión continua del riesgo, el diseño e implementación de controles y la aplicación de las Líneas de Defensa con el esquema de responsabilidades definida, integrando la prevención del riesgo de manera articulada e interrelacionada para lograr el mejoramiento de los procesos y cumplir la misión del Instituto, fortaleciendo la cultura organizacional y el apoyo en la toma de decisiones.</p> <p>El Comité Institucional de Coordinación de Control Interno (CICCI) [Línea Estratégica] lidera y exhorta a la integración de la gestión del riesgo, en todos los niveles desde la planeación estratégica hasta el desarrollo de las actividades de los procesos y la toma de decisiones por parte del Comité. Se han definido directrices que permiten la identificación, el análisis, la valoración y el tratamiento de los riesgos que puedan afectar de manera negativa el cumplimiento de la misión, las políticas y los objetivos estratégicos de los procesos y del Sistema Integrado de Gestión (SIG).</p> <p>De la misma manera, el INM se compromete a gestionar la disponibilidad de recursos necesarios, a ejercer control y a realizar seguimiento sobre los diferentes tipos de riesgos mediante una efectiva administración de estos, soportada en el control, la revisión y la mejora continua.</p> <p>La metodología para la gestión del riesgo toma como referencia los lineamientos establecidos por el Departamento Administrativo de la Función Pública- DAFP (Versión vigente), la cual está detallada en el documento E-02-D-001 "Gestión del riesgo" y complementa la presente política.</p> <p>Aprobada en Comité Institucional de Coordinación de Control Interno del 2023-03-13.</p>

En la página web del INM se evidencia la publicación de la política a través del enlace: <https://inm.gov.co/web/instituto-nacional-de-metrologia-de-colombia/planeacion/programa-de-transparencia-y-etica-publica-26481/>

<p>Programa de Transparencia y ética pública</p> <p>Año 2024</p> <ol style="list-style-type: none"> 1. Consulta pública <ol style="list-style-type: none"> 1.1 Matriz de riesgos de corrupción – consulta pública 1.2 Política de la administración de los riesgos 1.3 Matriz PTEP INM - 2024 1.4 Documento PTEP INM - 2024 2. Después de consulta pública <ol style="list-style-type: none"> 2.1 Matriz de riesgos de corrupción 2.2 Política de la administración de los riesgos 2.3 Matriz PTEP INM - 2024 2.4 Programa de Transparencia y Ética Pública V2 2.5 Documento PTEP INM - 2024 	<p>POLÍTICA DE ADMINISTRACIÓN DE RIESGOS</p> <p>El Instituto Nacional de Metrología de Colombia (INM) está comprometido con la gestión continua del riesgo, el diseño e implementación de controles y la aplicación de las Líneas de Defensa con el esquema de responsabilidades definida, integrando la prevención del riesgo de manera articulada e interrelacionada para lograr el mejoramiento de los procesos y cumplir la misión del Instituto, fortaleciendo la cultura organizacional y el apoyo en la toma de decisiones.</p> <p>El Comité Institucional de Coordinación de Control Interno (CICCI) [Línea Estratégica] lidera y exhorta a la integración de la gestión del riesgo, en todos los niveles desde la planeación estratégica hasta el desarrollo de las actividades de los procesos y la toma de decisiones por parte del Comité. Se han definido directrices que permiten la identificación, el análisis, la valoración y el tratamiento de los riesgos que puedan afectar de manera negativa el cumplimiento de la misión, las políticas y los objetivos estratégicos de los procesos y del Sistema Integrado de Gestión (SIG).</p> <p>De la misma manera, el INM se compromete a gestionar la disponibilidad de recursos necesarios, a ejercer control y a realizar seguimiento sobre los diferentes tipos de riesgos mediante una efectiva administración de estos, soportada en el control, la revisión y la mejora continua.</p> <p>La metodología para la gestión del riesgo toma como referencia los lineamientos establecidos por el Departamento Administrativo de la Función Pública- DAFP (Versión vigente), la cual está detallada en el documento E-02-D-001 "Gestión del riesgo" y complementa la presente política.</p> <p>Aprobada en Comité Institucional de Coordinación de Control Interno del 2024-01-25.</p>
--	--

Es importante resaltar que la política fue aprobada en la sesión 3 del Comité Institucional de Control Interno No. 1 el 31 de enero de 2024 que en ejercicio de los principios de efectividad, eficiencia y economía se realiza de manera conjunta con el CIGD; es importante indicar que no fue el 25 de enero de 2024, fecha en que se llevo a cabo la primera sesión.

IDENTIFICACIÓN DE RIESGOS

Con el propósito de determinar la cantidad de riesgos definidos en la entidad, se lleva a cabo una consulta en la hoja de mapa de procesos del archivo titulado <<Matriz de riesgos aprobación CIGD #1 2024-01-25>>, revelando un total de 130 riesgos discriminados de la siguiente manera:

- ✚ **Riesgos por proceso:** El siguiente cuadro muestra el número de riesgos asociados a cada uno de los procesos. La mayor cantidad de riesgos se concentra en la gestión de las tecnologías de la información, con 14 riesgos, lo que equivale al 10,77% del total. Le sigue la Administración del Sistema Integrado de Gestión, con 12 riesgos, representando el 9,23%. A continuación, la producción de materiales de referencia y el desarrollo de métodos analíticos cuentan con 11 riesgos, lo que equivale al 8,46%. Los servicios de calibración y medición metrológica presentan 10 riesgos, que representan el 7,69%, y los ensayos de aptitud tienen 9 riesgos, con una participación del 6,92%:

No.	ID	Descripción del proceso	Cantidad	% Total
1	A-01	Gestión Financiera	4	3,08
2	A-02	Defensa Judicial	2	1,54
3	A-03	Gestión Documental	3	2,31
4	A-04	Gestión de Talento Humano	5	3,85
5	A-05	Gestión Administrativa	4	3,08
6	A-06	Control Disciplinario	1	0,77
7	A-07	Contratación y Adquisición de Bienes y Servicios	4	3,08
8	A-08	Gestión de Servicios Metrológicos	8	6,15
9	C-01	Evaluación, acompañamiento y asesoría al Sistema de Control Interno	5	3,85
10	E-01	Direccionamiento Estratégico y Planeación	8	6,15
11	E-02	Administración del Sistema Integrado de Gestión	12	9,23
12	E-03	Comunicaciones	7	5,38
13	E-04	Servicio al Ciudadano	3	2,31
14	E-05	Gestión de las Tecnologías de la Información	14	10,77
15	M-01	Servicios de Calibración y medición metrológica	10	7,69
16	M-02	Capacitación, Formación y Cultura Metrológica	3	2,31
17	M-03	Producción de Materiales de Referencia y Desarrollo de Métodos Analíticos	11	8,46
18	M-04	Asistencia Técnica	3	2,31
19	M-05	Ensayos de Aptitud	9	6,92
20	M-06	Red Colombiana de Metrología	4	3,08
21	M-07	Investigación, Desarrollo e Innovación	3	2,31
22	M-08	Gestión de patrones nacionales y sistemas medición	7	5,38
TOTAL			130	100

✚ **Cantidad por tipo de riesgo** (Ordenado de mayor a menor) siendo el mayor el operativo con 68 y el menor el financiero con uno (1).

Tipo de riesgo	Cantidad
Operativo	68
Estratégico	32
Cumplimiento	7
Tecnológico	6
Confidencialidad	5
Gerencial	3
Imparcialidad	3
Seguridad digital	3
Fraude	2
Financiero	1
Total	130

Como se indicó con anterioridad, al realizar la consulta en Isolución se encontró un total de 130 riesgos “**Matriz DAFP**”. En la columna de referencia de la matriz de riesgos (A) en la hoja de excel se evidencia 133 registros lo que da a entender que corresponde a 133 riesgos, para corroborar y precisar la cantidad se realiza la verificación de la numeración en el archivo encontrándose que en la secuencia falta el número 99, 121 y 124 es decir, que corresponde a 130 riesgos y no a 133 lo cual guarda congruencia con el registro en Isolución.

Identificación del riesgo						
Referencia	ID	Proceso	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo
132	E05-R15	(E-05) Gestión de las Tecnologías de la Información	Económico y Reputacional	Desconocimiento por parte de los colaboradores del INM de las directrices establecidas por la entidad para la calificación de los activos de información Falta de compromiso por parte de los procesos de la entidad en la calificación de los activos de información Falta de liderazgo por parte del Profesional de Seguridad de la Información Aumento inesperado de contrataciones para la vigencia 2022.	Errorea identificación, clasificación y valoración del activo de información por parte del dueño y custodios de los activos de información	Posibilidad de afectación económica y reputacional al realizarse una inadecuada Calificación de la Confidencialidad, Integridad y Disponibilidad de la Información en la gestión de los Activos de información debido a una errónea identificación, clasificación y valoración del activo de información por parte del dueño y custodios de los activos de información
133	E05-R16	(E-05) Gestión de las Tecnologías de la Información	Económico y Reputacional	No existe una adecuada interrelación entre los diferentes procesos de la entidad con la ODT Algunos colaboradores y contratistas de la entidad utilizan los computadores personales	No se cuenta con licencias suficientes para otorgar dentro de la Suite de Google las cuentas de correo a los colaboradores del INM	Posibilidad de afectación económica y reputacional al afectarse la Seguridad de la información de la entidad (integridad, disponibilidad y confidencialidad) debido a no contar con licencias suficientes para asignar Google Suite a todos los colaboradores del INM

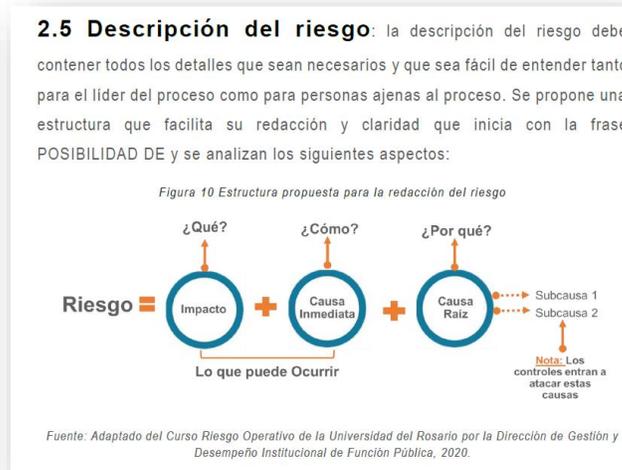
Frente a lo anterior, en una de las celdas de la matriz se encontró la siguiente anotación: “*Nota: La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. Una entidad puede ir en el riesgo 150 pero tener 70 riesgos,

lo que permite llevar una traza de los riesgos. Esta información la debe administrar la Oficina Asesora de Planeación o Gerencia de Riesgos.”

En cuanto a los riesgos No. 99, 121 y 124 en la pestaña denominada: “**control de cambios**” indica que estos riesgos son administrados desde la OIDT, con solicitud de cambio del 02 de abril de 2024.

CONTROL DE CAMBIOS		
FECHA Y RESPONSABLE DE LA SOLICITUD DE CAMBIO	CAMBIOS REALIZADOS	CIGD Y FECHA DE APROBACIÓN
2024-04-02: Correo electrónico enviado por parte de Liliانا Aponte para la OAP (Linda Karina Petro).	Riesgos de proceso. Se solicita por parte de la OIDT, la inclusión de los riesgos de proceso 06-1 (99), 05-17 (121) y 05-20 (124) para ser administrados desde la OIDT como tipología de riesgos de seguridad de la información. Dado lo anterior, los riesgos anteriormente mencionados pasan a ser administrados por parte de la OIDT como segunda línea para los riesgos de seguridad de la información.	Presentado en el CIGD # 6 del 2024-04-22 (sesión 1), no hubo necesidad de solicitar aprobación dado que los riesgos de seguridad de la información ya había sido aprobados previamente.

Considerando lo indicado en el numeral 2.5 descripción del riesgo de la guía del DAFT así:



Al verificar en la matriz la descripción de los 130 riesgos se encontró que 8 inician con el termino afectación económica, 98 posibilidad de, 11 posible pérdida o afectación y 13 inician con probabilidad de. Es decir, que 32 riesgos no fueron descritos con la frase “**posibilidad de riesgo**” como lo propone la guía.

Por otra parte, la estructura del riesgo incluye tres aspectos importantes dentro del cual se encuentra la “**causa inmediata**”, al consultarse en la matriz mediante un filtro se encontró que esta no se definió en seis (6) riesgos donde se registró un “**no aplica**” o **N.A.** La guía define la causa inmediata

como: "circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo".

A continuación, la imagen con lo descrito:

ID	Proceso	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo
M01-R0	Ordenar de A a Z		N.A.	Incumplimiento de las competencias técnicas requeridas para la prestación de servicios de calibración o medición	Afectación económica por suspensión temporal del servicio en curso por la ausencia respondido del personal subrogado para prestar el servicio programado o en ejecución debido al incumplimiento de las competencias técnicas requeridas para la prestación de servicios de calibración o medición	Ejecución y Administración de procesos
M01-R0	Ordenar de Z a A		N.A.	Incumplimiento de las competencias técnicas requeridas para la prestación de servicios de calibración o medición	Afectación económica por suspensión temporal del servicio en curso por la ausencia respondido del personal subrogado para prestar el servicio programado o en ejecución debido al incumplimiento de las competencias técnicas requeridas para la prestación de servicios de calibración o medición	Ejecución y Administración de procesos

Respecto a la causa raíz en comparación con el informe del año anterior emitido el 30 de mayo de 2023 en el cual se indicó: "La redacción de la causa raíz en algunos casos es errónea o incomprensible dado el factor distractor que suscitan textos o frases como por ejemplo la doble negación: "No contar con personal del laboratorio no disponible para la prestación del servicio". Se ratifica la observación puesto que al realizar el filtro en la matriz actual persiste el texto.

VALORACIÓN DE RIESGOS

Frente a la valoración del riesgo la guía establece:



Al realizar la consulta en la matriz de riesgos CIGD #1 2024-01-25 hoja mapa de procesos para los campos análisis de riesgos inherente (columna O a la U), evaluación del riesgo y valoración de los controles (columna V a AK) se identificó:

- Se evidencian los criterios para la definición del nivel de probabilidad para los 130 riesgos. (Muy baja 20%, baja 40%, media 60%, alta 80% y muy alta 100%) considerando la frecuencia de la actividad, asimismo, el impacto y la zona.
- En la hoja denominada "Matriz Calor Inherente" se identifica la zona para 11 de los 130 riesgos, es decir, para el 8,46%. La zona es el resultado del cruce de datos de la probabilidad e impacto definidos en cada riesgo. A continuación, la imagen con lo descrito:

Matriz de Calor Inherente		Impacto					
Probabilidad	Muy Alta 100%						Extremo
	Alta 80%						Alto
	Media 60%			R1 R2			Moderado
	Baja 40%			R13 R11 R3			Bajo
	Muy Baja 20%			R4 R5 R6 R7			
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%	

- Respecto a los controles se visualiza la definición de estos para los 130 riesgos, así como también la congruencia en términos generales con los lineamientos definidos en la Guía para la administración de riesgo y el diseño de controles en entidades públicas, incluyendo en la descripción responsable de ejecutar el control, la acción y el complemento, así como los atributos tanto de eficiencia (tipo, implementación) como informativos (documentación, frecuencia y evidencia).

Con el fin de realizar la verificación de los riesgos y sus controles para efectos de definir la muestra no se tendrán en cuenta aquellos procesos sobre los cuales dentro del plan anual de auditoria de la vigencia se tiene programada auditoria, es decir, para el proceso de Gestión de Servicios Metroológicos (A08) (ejecutada en abril y mayo) y Direccionamiento Estratégico y Planeación (E01).

Por otra parte, teniendo en cuenta que Gestión de las tecnologías de la información registra el mayor número de riesgos (14) y que adicionalmente este proceso fue auditado a finales de 2023 como consta en informe de auditoría expedido el 11 de diciembre de 2023 por la OCI donde se evaluaron los 16 riesgos existentes y se efectuaron las observaciones que se ratifican en el presente informe y que pueden ser consultadas a través de la página web de la entidad en el siguiente enlace: <https://inm.gov.co/web/wp-content/uploads/2024/02/Informe-Definitivo-de-auditoria-Gestion-de-las-Tecnologias-de-la-Informacion-E-05.pdf>

En cuanto a los demás procesos auditados en el segundo semestre de la vigencia 2023 tampoco se tendrán en cuenta para este análisis como el caso de: gestión del Talento Humano (2023-09-25), gestión de patrones nacionales (2024-02-12), gestión financiera (2023-11-24), gestión administrativa (2023-11-01) y contratación y adquisición de bienes (2024-01-19).

Considerando que el segundo lugar en cuanto al mayor número de riesgos corresponde a la Administración del Sistema Integrado de gestión con 12 riesgos y una participación del 9,23% sobre el total (130) a continuación se detallan los riesgos y sus controles para este proceso:

ID	Descripción del Riesgo	Descripción del Control
E02-R1	Posibilidad de afectación reputacional por el uso de documentos no oficiales (versiones obsoletas), cambio de normas o requisitos y otros documentos de referencia y por el desconocimiento del SIG por parte del personal de INM.	El responsable del proceso que elabora o actualiza un documento, garantiza que su personal conoce cuales son los documentos que se encuentran vigentes para el desarrollo de sus actividades a través de la solicitud a la OAP, del respectivo acceso a Isolución bien sea para la consulta o actualización de los documentos de su proceso. (Registro: Correo electrónico del jefe de proceso para el personal de la OAP)
		El responsable del proceso actualiza el listado maestro de documentos del proceso a través de Isolución al momento en que se crea o se crea una versión del documento (Registro: documento disponible desde listado maestro de documentos).
		El profesional designado en la OAP verifica que desde los procesos se hayan revisado y actualizado los requisitos legales o documentos externos aplicables al proceso, a través del envío de correo electrónico al personal de apoyo de calidad de cada proceso (Registro: Correo electrónico o matriz de seguimiento a requisitos legales/Docs. externos)
E02-R2	Posibilidad de afectación reputacional dada la pérdida de reconocimiento internacional por la ineficiencia en el cierre de acciones tomadas para la mejora en el instituto, por el	El profesional designado de la OAP consolida la información de las acciones tomadas por los responsables de los procesos, a través del seguimiento trimestral a estas acciones (Registro: E-02-F-015 Acciones correctivas y de mejora).

	desconocimiento de las acciones de cada uno de los planes de mejoramiento de los procesos debido a la falta lineamientos o recursos asignados por parte de la dirección para el cierre de los mismos y también porque al momento en que se genera un hallazgo transversal, se analizan y se generan acciones conjuntas sin los responsables de las áreas directamente involucradas en dicho hallazgo.	El responsable del proceso convoca a mesas de trabajo con el personal en los casos en que los hallazgos que requieran tomar acciones por parte de más de un proceso se convoca una mesa de trabajo para realizar el análisis de causas y definir las actividades del plan de mejoramiento, a través del correo electrónico (Registro: Citación a la reunión y la formulación de las Acciones de mejora). El profesional designado de la OAP revisa el cumplimiento y toma de decisiones por parte de los procesos del INM de manera trimestral, a través del informe presentado al CIGD y CICCI (Registro: Informe de seguimiento trimestral a las acciones de mejora).
E02-R3	Posibilidad de afectación reputacional dada la inadecuada identificación de las causas raíces para el cierre definitivo de hallazgos por realizar un análisis superficial en la identificación de acciones sobre los hallazgos debido a la participación limitada de los responsables de los procesos en la identificación de causas y acciones contundentes para solucionar los inconvenientes.	El responsable del área revisa uno a uno los planes de mejoramiento (análisis de causas, acciones formuladas, tiempos establecidos y entregables) al interior área a través de mesas de trabajo internas con el personal involucrado en dichos planes de mejora. El equipo de trabajo relacionado con el hallazgo analiza la causa raíz y análisis de impacto (cuando son no conformidades), a través de mesas de trabajo internas con el personal involucrado en dichos planes de mejora.
E02-R4	Posibilidad de afectación reputacional dado el incumplimiento de compromisos y objetivos de los procesos por incumplir con los lineamientos definidos en los documentos transversales establecidos en las áreas, debido a la falta de participación en la elaboración o actualización de estos documentos de las personas involucradas en el proceso pero que no pertenecen al área responsable de la gestión del mismo y a la falta de socialización de actualizaciones a los documentos transversales entre los involucrados en el desarrollo de las actividades del proceso.	El responsable del proceso de que elabora o actualiza documentos revisa la adecuación del documento antes de su aprobación, a través de la validación del contenido una vez haya finalizado este proceso de elaboración o actualización del documento, teniendo en cuenta la matriz de responsabilidades del procedimiento E-02-P-001 Control de documentos. El responsable del proceso de que elabora o actualiza documentos socializa las actualizaciones o nuevas versiones de los documentos al personal que tiene afectación directa sobre las actividades que en ese documento se describen, a través de la creación de mesas de trabajo o agendamiento sobre el calendario de google. Registro: Evidencia de asistencia y teniendo en cuenta el procedimiento E-02-P-001 Control de documentos. El responsable de documentar el plan de mejoramiento para el proceso convoca a mesas de trabajo a los distintos procesos involucrados en una actividad definiendo los roles, responsables y actividades a desarrollar, mediante las citaciones desde google calendario.
E02-R5	Posibilidad de afectación reputacional por proyectos implementados inconclusos, generados por la Implementación deficiente de actividades de Gestión del Cambio debido a la no identificación o identificación deficiente de los impactos que podría generar la implementación de	El responsable del proceso que propone el cambio (Subdirector, Jefe o Secretario General) revisa el impacto que tendría para su proceso la implementación del cambio a través del formato E-02-F- 042 de Solicitud del Cambio y lo aprueba o desaprueba según necesidades del área (Formato de Solicitud del cambio cargado en Isolución)

	<p>cambios en el instituto, en aspectos como el Sistema de Gestión, el presupuesto, los colaboradores, los procesos y los servicios, entre otros, o por la falta de seguimiento o seguimientos inadecuados en la implementación de actividades que generan cambios en el Instituto</p>	<p>Cambio de alto impacto: El Responsable del proceso que propone el cambio (Subdirector, Jefe o Secretario General) presenta resultados de avance trimestral en CIGD (Registro: Acta CIGD / Avance de actividades Isolución)</p> <p>Cambio de mediano impacto: El Responsable del proceso de Administración del SIG presenta resultados de avance trimestral en CIGD (Registro: Acta CIGD / Avance de actividades Isolución)</p> <p>Cambio de bajo impacto: El Responsable del proceso que propone el cambio (Subdirector, Jefe o Secretario General) hace seguimiento al estado y cierre de los planes de trabajo para implementar el cambio (Avance de actividades Isolución)</p>
E02-R6	<p>Posibilidad de afectación reputacional por pérdida de la oportunidad de identificación de situaciones claves para el mejoramiento de los procesos generados por la deficiente descripción de hallazgos de auditoría, debido a Inadecuada selección de auditores y/o expertos técnicos que realizan o acompañan la realización de auditorías de Gestión y por la falta de revisión de hallazgos de auditoría previa a la entrega del informe final de auditoría</p>	<p>El Profesional del proceso de Administración de SIG valida las competencias del personal disponible para realizar las auditorías (Revisor por Pares o auditor interno), de manera que se escojan las personas que cumplan las competencias requeridas para la realización de las auditorías, para lo cual solicita al auditor soportes (hoja de vida) de su experiencia como auditor, (Registro: formato E-02-F-035 Matriz de Auditores)</p> <p>El Profesional del proceso de Administración de SIG y/o el Apoyo de Calidad designado, analiza y valida el Informe Preliminar o registro de hallazgos de Auditoría, antes de efectuar la reunión de cierre, en caso de identificar inconsistencias o errores los comunica al equipo auditor para su análisis y discusión (Registro: Correo electrónico)</p>
E02-R7	<p>Posibilidad de afectación reputacional por pérdida de credibilidad por parte de evaluadores internacionales en la consistencia del SIG del INM, generada por la necesidad de evitar que se evidencien errores críticos dentro de los procesos, debido a la solicitud de no incluir hallazgos críticos por parte de personas auditadas y por la inadecuada selección de auditores y/o expertos técnicos que realizan o acompañan la realización de auditorías de Gestión</p>	<p>Los apoyos de Calidad y en ocasiones el Profesional del proceso de Administración de SIG acompañan la realización de las auditorías para tener conocimiento de los hallazgos levantados y asegurar que se incluyen dentro del informe final de auditoría</p> <p>El Profesional del proceso de Administración de SIG valida las competencias del personal disponible para realizar las auditorías (Revisor por Pares o auditor interno), de manera que se escojan las personas que cumplan las competencias requeridas para la realización de las auditorías, para lo cual solicita al auditor soportes (hoja de vida) de su experiencia como auditor, (Registro: formato E-02-F-035 Matriz de Auditores)</p>
E02-R8	<p>Posibilidad de afectación reputacional por ocurrencia de trabajos no conformes que no aseguran que se vuelva a presentar la situación presentada, generada por falta de análisis profundo de las situaciones que generaron los hallazgos, debido a la aplicación de acciones débiles o poco eficaces o a la falta de seguimiento de la puesta en operación de las acciones propuestas</p>	<p>El Coordinador del área o responsable del laboratorio efectúa seguimiento y apoya la realización de análisis para la generación de Trabajos No Conformes y lo aprueba o desaprueba según resultados de los análisis realizados (Registro: E-02-016 Ficha de trabajo no conforme)</p>

	<p>Posibilidad de afectación reputacional por ocurrencia de trabajos no conformes que no aseguran que se vuelva a presentar la situación presentada, generada por falta de análisis profundo de las situaciones que generaron los hallazgos, debido a la aplicación de acciones débiles o poco eficaces o a la falta de seguimiento de la puesta en operación de las acciones propuestas</p>	<p>El Profesional del proceso de Administración de SIG realiza evaluación, monitoreo y cierre del TNC, a través del registro de la información en el aplicativo Isolución (Registro: información cargada en Isolución relacionada con el TNC)</p>
<p>E02-R9</p>	<p>Posibilidad de afectación reputacional por fuga de Información valiosa para el INM, y que puede llegar a tomarse como oficial estando desactualizada o con posibilidad de ser modificada, debido a la entrega de información técnica a entidades externas o proveedores externos de servicios que para la realización de su actividad requieran de la información técnica del INM o cuando se realizan enmendaduras (cambios) a los datos que ya se haya incluido en un registro electrónico</p>	<p>Control: Firma por parte de los terceros de un compromiso de confidencialidad e imparcialidad. Periodicidad: Cada vez que se realiza una auditoría o evaluación por parte de un externo. Propósito: Cláusula por la cual se deben abstener de utilizar o divulgar la información recibida. Cómo: Cuando un Auditor o evaluador obtiene información del Instituto, realiza la firma de compromiso de confidencialidad e imparcialidad. Responsable: Profesional de la Oficina Asesora de Planeación. Desviaciones/Observaciones: 1. Si se presenta inconvenientes en la forma del compromiso, se procede a buscar un nuevo auditor/evaluador. 2. Si no se presentan inconvenientes, se obtiene la firma como compromiso o acuerdo ejecutable. Evidencia: Compromiso de auditores. Documento: Procedimiento de Auditorías Internas</p> <p>Control: Enmendaduras a los datos. Periodicidad: Cada vez que se haga una enmendadura a los datos registrados. Propósito: Garantizar que los registros se controlan incluyendo sus modificaciones. Cómo: Mediante la hoja de control de cambios. Responsable: Responsable de los procesos (Coordinadores o Responsables de área, colaboradores). Desviaciones/Observaciones: En los casos en que se detecte que se incluyen modificaciones, el responsable del Laboratorio debe revisar que la hoja de enmendaduras se diligencie con los cambios respectivos. Evidencia: Hoja de control de registros. Documento: Procedimiento Control de Registros</p>
<p>E02-R10</p>	<p>Posibilidad de afectación reputacional por insatisfacción de clientes y pérdida de la confidencialidad e integridad de la información debido al desconocimiento del SIG.</p>	<p>Control: Socialización de documentos. Periodicidad: Cada vez que se actualice un documento. Propósito: Garantizar el conocimiento de los documentos vigentes de los procesos al personal que los ejecuta. Cómo: Responsable: Responsable de los procesos (Coordinadores o Responsables de área). Desviaciones/Observaciones: 1. Si se presenta inasistencia de los colaboradores a las capacitaciones, el superior inmediato garantiza la entrega de la información a dichos colaboradores. 2. Si se presentan fallas técnicas que impidan la realización de la capacitación, ésta se debe reprogramar. Evidencia: Lista de asistencia de socialización de documentos del SIG o pantallazo de asistencia en caso</p>

		de ser virtual Documento: Procedimiento Control de Documentos.
E02-R11	Posibilidad de afectación reputacional por incumplimiento de requisito del Sistema de Gestión e inadecuada toma de decisiones por debilidades en la comunicación con los procesos y la desorganización en la entrega de información dentro del tiempo establecido requerida por todos los procesos para la revisión por la dirección .	Control: Reuniones previas de trabajo con los apoyos de calidad. Periodicidad: Cada vez que se realice la revisión por la dirección Propósito: Garantizar que se comunica a todos los involucrados de los procesos, la fecha de solicitud de la información y el periodo evaluado, y la información a remitir. Cómo: AJUSTAR Responsable: Profesional de la Oficina Asesora de Planeación Desviaciones/Observaciones: 1. Si no se allega información dentro del plazo previsto se reitera la solicitud y se habla con el responsable del proceso. Evidencia: Correo electrónico con la solicitud. Documento: Procedimiento revisión por la dirección.
E02-R12	Posibilidad de afectación reputacional por la pérdida de las Certificaciones obtenidas anteriormente (5 años) debido al incumplimiento de los requisitos y a los tiempos establecidos cuando requiere presentarse el SIG al QSTF por cierre de hallazgos o información inadecuada o incompleta	Control: Consolidar el seguimiento de las acciones Periodicidad: trimestralmente. Propósito: Asegurar cumplimiento de la acción formulada y verificar la coherencia de las evidencias de las acciones cerradas frente a las causas y hallazgos Cómo: Recibe la información y consolida los seguimientos realizados por los responsables de los procesos. Valida la evidencia en cumplimiento de las acciones. Responsable: Profesional de la Oficina Asesora de Planeación Desviaciones/Observaciones: Si la evidencia da cumplimiento al cierre de la acción lo confirma al colaborador que remitió el avance. Si la evidencia no da cumplimiento al cierre de la acción lo devuelve al colaborador que remitió el avance. Evidencia: Consolida los reportes de cada uno de los procesos E-02-F-015 Acciones Correctivas y de Mejora, diligenciado con comentarios o avances (planes antes del 2020) y genera informe de ISOLUCION con el avance de las acciones. Documento: Procedimiento E-02-P-003 Acciones correctivas y de mejora.

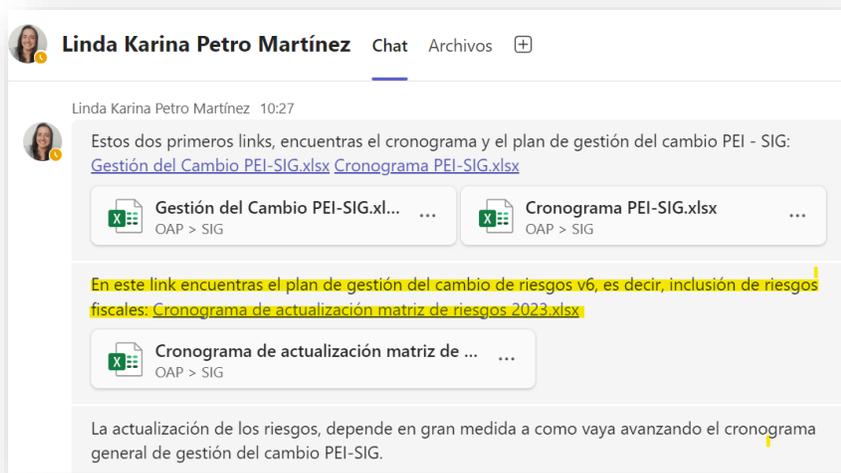
		<p>Control: Lineamientos para presentación y publicación de CMC.</p> <p>Periodicidad: Cada vez que se programe la presentación de CMC</p> <p>Propósito: Verificar los documentos e información recolectada para QSTF</p> <p>Cómo:</p> <p>Responsable: Profesional de la Oficina Asesora de Planeación</p> <p>Desviaciones/Observaciones: 1. Si la evidencia da cumplimiento a los registros y formularios del QSTF envía la documentación al secretario del QSTF. 2. Si la evidencia no da cumplimiento se informa a la Alta Dirección la decisión de no presentar sistema integrado de gestión.</p> <p>Evidencia: QSTF 3</p> <p>Documento: Lineamientos para presentación y publicación de CMC.</p>
--	--	--

En cuanto a los controles no se tiene ninguna observación en cuanto a su diseño. Es importante aclarar que esta verificación no incluye la verificación del cumplimiento de los controles sin embargo al consultar en la matriz se registro el seguimiento por parte de la profesional Linda Karina Petro el 8 y 9 de abril de 2024 indicando que ninguno de los riesgos se materializó de acuerdo con la columna J de la pestaña "**seguimiento**".

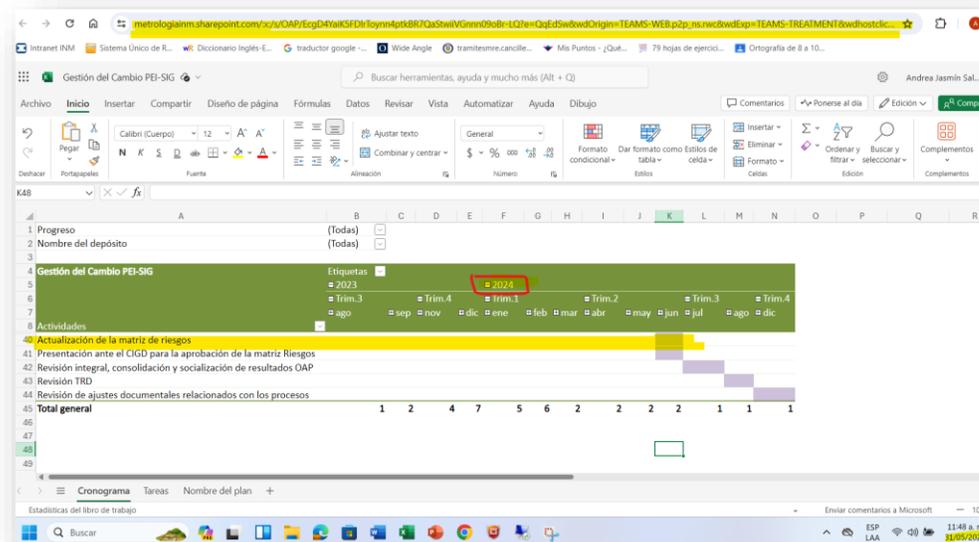
LINEAMIENTOS PARA EL ANÁLISIS DE RIESGO FISCAL

Al realizar la consulta en la matriz de riesgos de la entidad no se identifica en la clasificación riesgos fiscales como se indicó en el informe del año anterior. Al consultar en Isolucion el alcance del documento gestión del riesgo E-02-D-001 versión 4 del 25 de abril de 2023 indica: "*Aplica para todas las actividades desarrolladas por el INM en todos sus niveles y los riesgos asociados a éstas, cubriendo tanto los procesos, como proyectos institucionales y programas especiales. Incluye la gestión de los riesgos institucionales, riesgos de corrupción y de seguridad de la información*". (Negrilla fuera de texto). Es decir, que no se encuentran establecidos dentro del sistema integrado de gestión.

Por lo anterior, se procede a consultar a la profesional Linda Karina Petro de la Oficina Asesora de planeación a través del chat institucional respecto a la existencia o no de estos riesgos, frente a lo cual la funcionaria indica que aún no, pero en el marco del plan de gestión del cambio PEI-SIG y del plan de cambio de gestión del riesgo se incluye los riesgos fiscales, como soporte de lo indicado comparte información a la OCI como se muestra a continuación:



Adicionalmente, comparte “la carpeta completa de los documentos en estado de borrador” sobre los cuales se esta realizando el proceso de actualización. Al consultar este material se encontró entre otros el cronograma para la actualización de la matriz de riesgos y el catálogo indicativo y enunciativo de puntos de riesgo fiscal y circunstancias inmediatas anexo 1 de la Función Pública como se detalla en las siguientes imágenes:



Así las cosas, como resultado del análisis de más de 130 fallos con responsabilidad fiscal tanto de contralorías territoriales como de la Contraloría General de la República, fue posible identificar 50 puntos de riesgo fiscal e igual número de circunstancias inmediatas, así:

Id Referencia	Puntos de Riesgo Fiscal <i>Actividad en la que potencialmente se origina el riesgo fiscal</i>	Circunstancia Inmediata <i>Situación por la que se presenta el riesgo</i>	PROCESOS EN EL INM CON POSIBLE IMPACTO
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción	
2	Cumplimiento de obligaciones	Pago de Intereses moratorios	
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente	
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos	
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados	
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad	
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público	

Es importante que se tenga presente que el riesgo fiscal es la posibilidad de incurrir en pérdidas financieras o sanciones debido a errores, incumplimientos o interpretaciones incorrectas de las leyes fiscales y regulaciones tributarias. Identificar el riesgo fiscal es crucial para las organizaciones por varias razones:

- ✓ **Cumplimiento legal:** Identificar los riesgos fiscales ayuda a garantizar que se cumpla con todas las leyes y regulaciones fiscales vigentes, evitando así posibles sanciones y multas por incumplimiento.
- ✓ **Optimización fiscal:** Al identificar los riesgos fiscales, la entidad puede tomar medidas proactivas para optimizar su situación fiscal, aprovechando al máximo las oportunidades de deducciones, exenciones y beneficios fiscales disponibles.
- ✓ **Planificación estratégica:** La identificación de riesgos fiscales permite planificar estratégicamente sus actividades misionales así como financieras, anticipando posibles implicaciones fiscales y tomando decisiones informadas para minimizar el impacto fiscal.
- ✓ **Gestión de la reputación:** Evitar controversias fiscales y escándalos ayuda a proteger la reputación y la imagen de la empresa ante clientes, inversores y otras partes interesadas.
- ✓ **Reducción de costos:** La gestión efectiva de los riesgos fiscales puede ayudar a reducir los costos asociados con auditorías, litigios fiscales y posibles penalizaciones, lo que contribuye a la eficiencia como uno de los principios rectores de la gestión pública.

RIESGOS DE CORRUPCIÓN

En el presente informe no se hará énfasis en los riesgos de corrupción debido a que estos fueron abordados en el seguimiento programa de transparencia y ética pública con corte al 30 de abril expedido el 14 de mayo de 2024 en el cual se incluyeron las siguientes recomendaciones por parte de la OCI:

6. RECOMENDACIONES

- 6.1** Realizar procesos de capacitación a todo el personal de la entidad sobre el nuevo componente "Medidas de debida diligencia y prevención del lavado de activos".
- 6.2** Promover campañas al interior de la entidad con el fin de prevenir actos de corrupción por parte de los funcionarios públicos y en general del personal al interior del Instituto. Las campañas pueden incluir entre otros aspectos los siguientes:
 - **Comunicación clara de valores y políticas:** socialización de los valores del código de ética del funcionario público y de los que haya establecido la entidad.
 - **Capacitación y sensibilización:** Ofrecer programas de capacitación sobre ética, integridad y prevención de la corrupción a todos los empleados de la entidad es esencial. Estos programas deben enfocarse en la identificación de comportamientos corruptos, las consecuencias legales y éticas de la corrupción, y cómo reportar posibles irregularidades de manera segura.
 - **Promover de manera permanente y segura los canales de denuncia** con el fin de que los funcionarios públicos o cualquier otra persona pueda reportar actos de corrupción de manera anónima y sin temor a represalias.
 - **Monitoreo y evaluación continua:** Realizar un seguimiento regular del impacto de las campañas anticorrupción y evaluar su efectividad mediante encuestas de clima laboral, métricas de denuncias recibidas y casos resueltos.

Adicionalmente, al consultar la matriz de riesgos de corrupción que se encuentra en el mismo archivo de los riesgos de proceso denominado: "matriz de riesgos aprobación CIGD # 1 2024-01-25" se encontraron 17 riesgos de corrupción los cuales difieren de los que se encuentran cargados en la pestaña "**Riesgos corrupción**" en Isolucion que refiere 119 como se evidencia en la siguiente imagen:

Núm.	Nombre	Caso de Riesgo	Etapo	Fecha de Creación	Responsable	Proceso	Causa	Consecuencia
01-1	Ausencia de los instrumentos, patrones requeridos en la prestación del servicio	Operativo	Valoracion	09/feb./2021	Linda Karina Petro Martínez	Servicio de Calibración y Medición Metrología	Demora en la prestación del servicio por parte de otro instituto. Incumplimiento de plazo de reimportación de equipos por la agencia aduanera. Incumplimiento en la entrega de equipos por parte de la empresa transportadora	*Reclamaciones o quejas de los usuarios. *Reprogramaciones de servicios *Demoras en la prestación de servicios
01-2	Daños en los instrumentos o equipos de medición durante el proceso de transporte	Operativo	Control	10/feb./2021	Linda Karina Petro Martínez	Servicio de Calibración y Medición Metrología	Inconvenientes o imprevistos en el proceso de transporte	* Daño del instrumento * Cancelación del servicio asociado al instrumento * Suspensión del servicio asociado al instrumento
01-3	Demora en la prestación del servicio de calibración.	Operativo	Control	10/feb./2021	Linda Karina Petro Martínez	Servicio de Calibración y Medición Metrología	Condiciones ambientales del laboratorio fuera de los límites establecidos. Personal del laboratorio no disponible para la prestación del servicio	*Atraso en los demás servicios prestados por el laboratorio *Incumplimiento a la programación de la prestación del servicio de calibración *Imagen negativa por parte del cliente por presentar retrasos en la prestación del servicio.
01-4	Ocurriencia de un evento adverso, durante la prestación del servicio de calibración o medición.	Operativo	Control	10/feb./2021	Linda Karina Petro Martínez	Servicio de Calibración y Medición Metrología	Recibo de instrumento con daño oculto. Falta de información sobre operación del instrumento. Manipulación inadecuada del ítem de calibración por falta de experiencia del personal técnico. Ausencia de instrucciones para la manipulación de los IBC.	*Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. * Reclamaciones o quejas de los usuarios *Reclamaciones ante empresas aseguradoras por parte del cliente o del INM. *Intervención de las Aseguradoras de Riesgos Profesionales
01-5	El certificado de calibración es firmado por una persona no autorizada para realizar la labor	Operativo	Valoracion	10/feb./2021	Linda Karina Petro Martínez	Servicio de Calibración y Medición	El laboratorio no cuenta con el personal suficiente para la revisión del certificado. La persona que revisa el certificado de calibración no fue entrenado.	* El certificado de calibración puede ser revisado por una persona no calificada, lo cual puede que no se detecten posibles errores. * Si el usuario recibe un certificado con errores se pueden presentar quejas al servicio. * Se debe

En la columna “Clase de riesgo” no solo se encuentran los de corrupción menciona otros como: operativo, tecnológico 2, estratégico, imparcialidad 1, financiero entre otros). Lo indicado, denota falta de uniformidad, estandarización y consistencia entre las diferentes fuentes de información, lo cual puede llevar a los usuarios de la información a errores, confusiones, dificultades para la comparación, duplicidad de esfuerzos, retrasos en el procesamiento y análisis de la información.

LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Frente a los lineamientos definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas el 30 de mayo de 2024 se solicitó a través de correo electrónico a la Oficina de Informática y Desarrollo Tecnológico (OIDT) la matriz de riesgos de seguridad de la información vigente en la cual se identificó:

✓ Riesgos

A continuación, se muestran los 27 riesgos incluidos en la matriz:

Referencia	Proceso	Descripción del riesgo	Clasificación del riesgo	Tipo de riesgo
1	(E-03) Comunicaciones	La ausencia de gestión de contraseñas de redes sociales puede ocasionar un acceso no autorizado, lo que causaría la pérdida de la integridad de la información publicada en redes sociales.	Usuarios, productos y prácticas organizacionales	Seguridad digital
2	(A-05) Gestión Administrativa	Probabilidad de error humano en el registro de inventario de activos debido a que la actividad se lleva de forma manual, lo que podría causar la pérdida de integridad de la información	Usuarios, productos y prácticas organizacionales	Seguridad digital
3	(A-06) Control Disciplinario	La inadecuada custodia y manejo de los documentos y carpetas que hacen parte de los expedientes y la ausencia de controles fuertes de acceso físico pueden ocasionar el hurto de expedientes o piezas procesales lo que causaría la pérdida de la confidencialidad de la información de procesos disciplinarios	Ejecución y Administración de procesos	Seguridad digital

4	(E-05) Gestión de las Tecnologías de la Información	La ausencia de capacitación de personal en el manejo de phishing, ausencia de monitoreo de seguridad, ausencia de backups, ausencia de segmentación en la redes y ausencia de actualización de software de sistema operativo, facilita la posibilidad de un secuestro de información, lo cual causaría la pérdida de disponibilidad y confidencialidad de la información de los servicios	Ejecución y Administración de procesos	Seguridad digital
5	(E-05) Gestión de las Tecnologías de la Información	Ausencia de herramientas de seguridad, ausencia de monitoreo de seguridad y ausencia de políticas de seguridad de la información del personal pueden ocasionar la intrusión de un ataque informático, lo que puede causar la pérdida de disponibilidad de la información en los servidores	Ejecución y Administración de procesos	Seguridad digital
6	(E-05) Gestión de las Tecnologías de la Información	La ausencia de monitoreo de seguridad y ausencia de herramientas de seguridad informática puede ocasionar que ocurra una denegación de un servicio, lo cual causa la pérdida de disponibilidad de la información de los servicios	Fallas Tecnológicas	Seguridad digital
7	(E-05) Gestión de las Tecnologías de la Información	El uso de contraseñas débiles, la ausencia de políticas de seguridad en el manejo de credenciales, no cumplimiento de procedimientos de gestión de usuarios y ausencia de inscripción en la autenticación permite accesos no autorizados a la información, lo cual causaría la pérdida de la confidencialidad de la información de los sistemas internos	Fallas Tecnológicas	Seguridad digital
8	(E-05) Gestión de las Tecnologías de la Información	La ausencia de autenticación fuerte permite accesos no autorizados a la información, lo cual causaría la pérdida de la confidencialidad de ésta en servicio en línea	Fallas Tecnológicas	Seguridad digital
9	(E-05) Gestión de las Tecnologías de la Información	Ausencia de supervisión de derechos de acceso, la falta de capacitación del personal en políticas de seguridad de la información y la ausencia de obligación contractual del cumplimiento de políticas de seguridad de la información puede ocasionar que se ejecute un acto fraudulento, lo que causaría la pérdida de la integridad de la información de los servicios	Fraude Interno	Seguridad digital

10	(E-05) Gestión de las Tecnologías de la Información	La ausencia de gestión de capacidad, obsolescencia de equipos y ausencia de alta disponibilidad de la infraestructura tecnológica puede ocasionar una falla en el servicio, lo que causa la pérdida de disponibilidad de la información de los servidores	Fallas Tecnológicas	Seguridad digital
11	(A-05) Gestión Administrativa	Ausencia de respaldo de la planta eléctrica, fallas del proveedor de servicio de energía ocasionan la no disponibilidad de los servicios del datacenter, por lo cual hay pérdida de disponibilidad de todos los servicios del INM que están en las instalaciones	Fallas Tecnológicas	Seguridad digital
12	(E-05) Gestión de las Tecnologías de la Información	Ausencia de plan de continuidad del negocio, sitio alternativo y backups fuera del INM, ocasiona la pérdida de información frente al impacto de un desastre natural que afecte el Datacenter, lo cual causa la pérdida de la disponibilidad de los servicios en el datacenter del INM	Daños Activos Físicos	Seguridad digital
13	(E-05) Gestión de las Tecnologías de la Información	Gestión de derechos de usuario y asignación de recursos no adecuada y/o uso de contraseñas débiles puede ocasionar que haya accesos no autorizados a las aplicaciones, lo que ocasionaría la pérdida de confidencialidad de la información del directorio activo	Ejecución y Administración de procesos	Seguridad digital
14	(E-05) Gestión de las Tecnologías de la Información	Ausencia políticas de backups y falta de recursos para backups puede ocasionar que no se respalde adecuadamente la información crítica, lo que causaría la pérdida de disponibilidad de la información de copias de respaldo	Ejecución y Administración de procesos	Seguridad digital
15	(M-08) Gestión de patrones nacionales y sistemas medición	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, omisión de la aplicación de los lineamientos de seguridad digital y control de acceso, contraseñas sin protección y mecanismos de autenticación débil, puede facilitar la modificación no autorizada, lo cual causaría la pérdida de la integridad de información de los registros técnicos que evidencia la actividad del laboratorio para la gestión de los patrones y sistemas de medición.	Ejecución y Administración de procesos	Seguridad digital

16	(M-01) Servicios de Calibración y medición metrológica	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, omisión de la aplicación de los lineamientos de seguridad digital y control de acceso, contraseñas sin protección y mecanismos de autenticación débil, puede facilitar la modificación no autorizada, lo cual causaría la pérdida de la integridad de información de los registros técnicos que evidencia las actividades del laboratorio para la prestación de los servicios de calibración y medición.	Ejecución y Administración de procesos	Seguridad digital
17	(M-01) Servicios de Calibración y medición metrológica	La ausencia de procesos de verificación de información y ausencia de capacitación al personal en sus funciones puede ocasionar errores humanos en el manejo de los certificados de calibración, lo que causaría la pérdida de integridad de este en SAMS	Ejecución y Administración de procesos	Seguridad digital
18	(M-08) Gestión de patrones nacionales y sistemas medición	La ausencia de mantenimiento a los equipos puede ocasionar la falla del equipo, lo que causaría una pérdida de disponibilidad de los equipos esclavos de los laboratorios	Fallas Tecnológicas	Seguridad digital
19	(M-08) Gestión de patrones nacionales y sistemas medición	La ausencia de protección de seguridad, pueden ocasionar acceso no autorizados a la información, lo que causaría una pérdida de confidencialidad de la información en los equipos de cómputo esclavos de los laboratorios	Ejecución y Administración de procesos	Seguridad digital
20	(M-07) Investigación, Desarrollo e Innovación	La Gestión no adecuada de disposición del a información sensible en los repositorios definidos por la entidad y la ausencia de gestión de restricciones a las carpetas compartidas puede ocasionar un acceso no autorizado a dicha información y puede causar una pérdida de confidencialidad de los proyectos de investigación, desarrollo e innovación	Ejecución y Administración de procesos	Seguridad digital
21	(A-07) Contratación y Adquisición de Bienes y Servicios	La Gestión no adecuada de disposición del a información sensible en los repositorios definidos por la entidad y la ausencia de gestión de restricciones a las carpetas compartidas puede ocasionar un acceso no autorizado a dicha información y puede causar una	Ejecución y Administración de procesos	Seguridad digital

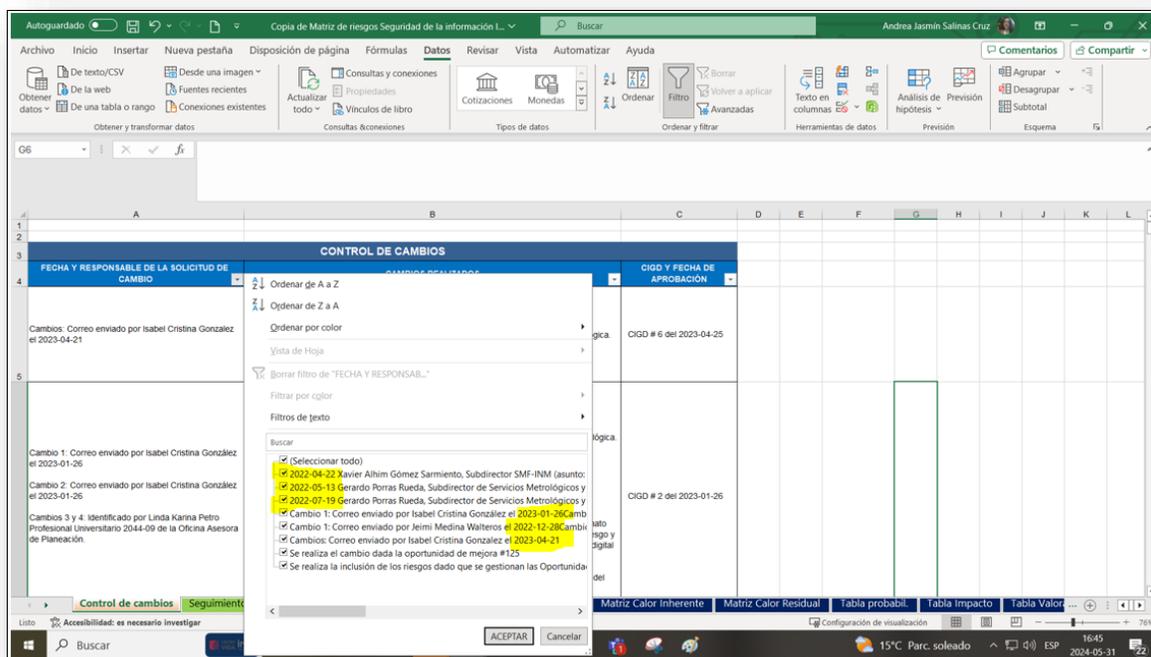
		pérdida de confidencialidad de la información de contratos.		
22	(A-04) Gestión de Talento Humano	La Gestión no adecuada de disposición de información confidencial reservada alta en los repositorios definidos por la entidad, puede ocasionar un acceso no autorizado, lo que puede causar la pérdida de confidencialidad de datos sensibles de los empleados contenidos en la matriz demográfica	Ejecución y Administración de procesos	Seguridad digital
23	(A-04) Gestión de Talento Humano	La Gestión no adecuada de disposición de información sensible en los repositorios definidos por la entidad y la ausencia de definición de políticas de retención adecuada, puede ocasionar pérdida de información y puede causar una pérdida de disponibilidad de la información de historias laborales	Ejecución y Administración de procesos	Seguridad digital
24	(E-03) Comunicaciones	La ausencia de gestión adecuada de publicación de la información de la página web puede ocasionar la exposición de información confidencial, lo que causaría una pérdida de confidencialidad de la información en la página web	Ejecución y Administración de procesos	Seguridad digital
25	(E-02) Administración del Sistema Integrado de Gestión	La ausencia de monitoreo de disponibilidad del sistema de información Isolucion puede ocasionar que haya fallas de conexión, lo que causa la pérdida de disponibilidad de la información en Isolucion	Fallas Tecnológicas	Seguridad digital
26	(E-02) Administración del Sistema Integrado de Gestión	Por uso de contraseñas débiles en Isolucion puede ocurrir un acceso autorizado a la información, lo que causaría una pérdida de integridad de la información en Isolucion	Ejecución y Administración de procesos	Seguridad digital
27	(E-02) Administración del Sistema Integrado de Gestión	Por la ausencia de gestión de privilegios de la información, puede ocurrir un acceso no autorizado lo que causaría una pérdida de confidencialidad de la información de auditorías externas e internas	Ejecución y Administración de procesos	Seguridad digital

Al realizar el seguimiento de la incorporación de los tres (3) riesgos de procesos con referencia Nos. 99, 121 y 124 no fue posible identificarlos en esta matriz considerando lo indicado en el control de cambios de la matriz de riesgos de procesos a la cual se hizo alusión en el conteo de riesgos por procesos en el presente informe.

Los tres (3) riesgos son los siguientes, según consulta realizada en el archivo denominado: "matriz de riesgos aprobación CIGD # 10 2023-07-18".

Identificación del riesgo				
ID	Proceso	Causa Inmediata	Causa Raíz	Descripción del Riesgo
09	A05-F01 (A-06) Control Disciplinario	Pérdida de expedientes o piezas procesales	Inadecuada custodia y manejo de los documentos y carpetas que hacen parte de los expedientes	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.
121	E05-F04 (E-05) Gestión de las Tecnologías de la Información	Ausencia o Desconocimiento de Políticas de Seguridad de la Información	Ataques Informáticos	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).
121	E05-F04 (E-05) Gestión de las Tecnologías de la Información	Ausencia de Controles de Acceso a la Información La entidad no cuenta con Herramientas Informáticas de Protección	Ataques Informáticos	Pérdida de disponibilidad de la información contenida en los servidores de la entidad debido a la ausencia de políticas de uso aceptable que pueden facilitar un espionaje remoto (ataque informático).
124	E05-F07 (E-05) Gestión de las Tecnologías de la Información	Ausencia o Desconocimiento de Políticas de Seguridad de la Información Ausencia de Controles de Acceso a la Información La entidad no cuenta con Herramientas Informáticas de Protección	Falta de herramientas informáticas que permitan la identificación y reconocimiento de ciber amenazas	Pérdida de disponibilidad de la información contenida en los servidores de la entidad debido a la ausencia de mecanismos de monitoreo para cerrar brechas de seguridad que puede producir fallas en los equipos por falta de herramientas informáticas que permitan la identificación y reconocimiento de ciber amenazas

Por otra parte, para efectos de confirmar la inclusión de los riesgos citados se realiza la consulta en el control de cambios de la matriz de seguridad de la información como se muestra a continuación:



Como se evidencia en la imagen no se registra ningún cambio realizado durante lo transcurrido de 2024, por cuanto es importante realizar la

verificación y el correspondiente registro sin perder la trazabilidad y el seguimiento de los riesgos definidos al interior de la entidad.

✓ **Identificación de los activos de seguridad de la información**

En la hoja de mapa de procesos de la matriz, se encuentran identificados los activos de información (columna K) detallados así: Información publicada en redes sociales, 210.150.2 inventario de bienes, 220.215.1 procesos disciplinarios, servicios, servidores, sistemas, servicio en línea, instalaciones, datacenter, directorio, herramientas, registros, SASM, equipo de computo esclavos de los laboratorios, proyectos de investigación, desarrollo e innovación, contratos, matriz socio demográfica, 240.125 historias laborales, página web, Isolucion, informes de auditorías externas 110.135.4 e informes de auditorías internas. No se observa si el Sistema de Seguimiento de Planes de Mejoramiento - SISEPM se encuentre dentro de estos activos.

K	L	M	N
Solo para riesgos clasificados como de Seguridad de la Información			
Activo de Información	Variable de Seguridad que Afecta	Amenaza	Vulnerabilidades
Información publicada en redes sociales	Pérdida de Integridad	Acceso no autorizado	Ausencia de gestión de contraseñas de redes sociales

Respecto a la identificación del riesgo, en la matriz (columna L) se encuentra definido, incluye tres (3), pérdida de disponibilidad, perdida de confidencialidad y perdida de integridad.

Además, al revisar detalladamente la hoja de cálculo en la matriz, se identificaron riesgos relacionados con la corrupción. Si bien el archivo consta de varias hojas, únicamente se debe incluir información relacionada con los riesgos de seguridad de la información. Las demás hojas no deberían contener datos adicionales, a menos que estén destinadas a la consolidación de los riesgos de la entidad.

Por otra parte, en la reunión que se llevó a cabo el 31 de mayo de 2024 a través de teams entre la OCI y la OAP (profesional especializado Yesid Javier Pineda) con el fin de dar continuidad a la revisión de la caracterización de control interno, indicadores y riesgos del proceso se evidenció que el riesgo No. 116 con ID C01-R4 "Posibilidad de Hallazgos de auditoría y reprocesos administrativo por pérdida de información del Sistema de Seguimientos de Planes de Mejoramiento debido a fallas de seguridad de la información" se puede clasificar como un riesgo de seguridad de la información y no como un riesgo de proceso.

Respecto a lo indicado, en el plan de mejoramiento 112 se observó que en el hallazgo **Código de Hallazgo 1 de 2022**, al proceder a registrar el seguimiento del corte del 31 de diciembre de 2024 y realizado el 24 de enero de 2024 en el SISEPM este no fue posible ya que presentaba seguimiento y aprobación por parte de la OCI sin que esta lo hubiese realizado, como se observa a continuación (pantallazo del día 24 de enero de 2024):

los saldos pendientes de recobro a la EPS por incapacidades, para lo cual sera necesario el trabajo conjunto entre Financiera y Talento humano, en el

No.	Fecha Registro	Observaciones Cumplimiento	Responsable	Fecha Seguimiento	Observaciones Seguimiento	Responsable	Estado
1	2024-01-09	Se anexa base de datos con la información consolidada de kactus	PATRICIA ANDREA AYALA BELTRAN				CREADO
2	2024-01-10	Actas de las conciliaciones realizadas	PATRICIA ANDREA AYALA BELTRAN	2024-01-15	Texto de prueba para ingresar observaciones correspondientes a la calificación o aprobación de un soporte	SANDRA LUCÍA LÓPEZ PEDREROS	APROBADO

Desde ese día se solicitó el debido ajuste y se indicó que no fue posible registrar comentario en SISEPM y que aparecía aprobado cuando esta tarea no fue realizada por la OCI.

Es esencial destacar que el 4 de marzo de 2024 se llevó a cabo la elaboración del informe titulado "ESTADO DE CUMPLIMIENTO PLAN DE MEJORAMIENTO CON LA CGR". Además, se observó que, a solicitud del funcionario Omar Mejía para habilitar el aplicativo SISEPM con el fin de cargar soportes, ya no se encontraba registrado el comentario del 15 de enero de 2024. Además, se detectó la presencia de cuatro comentarios adicionales supuestamente

realizados por la jefe de control interno, los cuales no fueron efectuados por ella. A continuación, se adjunta la imagen correspondiente:

1	2024-01-09	2024-01-09	Se anexa base de datos con la información consolidada de kactus	PATRICIA ANDREA AYALA BELTRAN	2024-02-16	Falta los Comprobantes contables de ajuste	SANDRA LUCÍA LÓPEZ PEDREROS	APROBADO	
2	2024-01-10	2024-01-10	Actas de las conciliaciones realizadas	PATRICIA ANDREA AYALA BELTRAN				CREADO	
3	2024-02-16	2024-02-16	asdfa sdf asdf asdfa sdf asdf asdf	SANDRA LUCÍA LÓPEZ PEDREROS	2024-02-16	Registrado por Control Interno	SANDRA LUCÍA LÓPEZ PEDREROS		
4	2024-02-16	2024-02-16	sadfasd fasdf asdf asdf asd	SANDRA LUCÍA LÓPEZ PEDREROS	2024-02-16	Registrado por Control Interno	SANDRA LUCÍA LÓPEZ PEDREROS		
5	2024-02-16	2024-02-16	asdfasdf	SANDRA LUCÍA LÓPEZ PEDREROS	2024-02-16	Registrado por Control Interno	SANDRA LUCÍA LÓPEZ PEDREROS		
6	2024-02-16	2024-02-16	sdfasdfasdf	SANDRA LUCÍA LÓPEZ PEDREROS	2024-02-16	Registrado por Control Interno	SANDRA LUCÍA LÓPEZ PEDREROS		

Estos eventos podrían desencadenar en riesgos potenciales que podrían incluir:

- ✓ **Manipulación de Datos:** La ausencia del comentario del 15 de enero de 2024 y la realización de numerosos comentarios falsos a nombre de la jefe de control interno indican la posibilidad de manipulación de datos. Esto puede comprometer la integridad de la información y afectar la confianza en los registros.
- ✓ **Falta de Seguridad en el Sistema:** La solicitud de habilitar el aplicativo para cargar soportes por parte del funcionario Omar Mejía podría implicar un riesgo de seguridad. Si no se tiene un control adecuado sobre quién puede acceder y realizar cambios en el sistema, se aumenta la posibilidad de manipulaciones indebidas.
- ✓ **Suplantación de Identidad:** La realización de comentarios a nombre de la jefe de control interno sin su consentimiento indica un riesgo de suplantación de identidad. Esto no solo afecta la integridad de la información, sino que también podría tener implicaciones legales y éticas.
- ✓ **Riesgos de Cumplimiento:** Podría implicar riesgos de incumplimiento con políticas internas, regulaciones externas o estándares de auditoría.

Es importante abordar estos riesgos de manera proactiva, y tomar medidas correctivas para garantizar la integridad y la confidencialidad de la información, así como para fortalecer los controles de seguridad y la autenticidad de los registros. Además, se puede considerar la implementación de medidas para prevenir futuros incidentes similares.

5. CONCLUSIONES

Como resultado de la verificación, se llega a las siguientes conclusiones:

- ✚ La política de riesgos y la matriz de riesgos fueron refrendadas y aprobadas durante la sesión 3 del CICCI No. 1, llevada a cabo el 31 de enero de 2024, como consta en la respectiva acta.
- ✚ Actualmente, el INM no cuenta con una matriz de riesgos fiscales. La Oficina Asesora de Planeación está en proceso de actualizar la matriz de riesgos de la entidad, de acuerdo con el cronograma y la inclusión de estos riesgos.
- ✚ Se detectó una discrepancia en los riesgos de corrupción registrados en Isolucion, donde se evidenció una cantidad de 119, en contraste con los 17 riesgos reales.
- ✚ No se pudo encontrar en la matriz de riesgos de seguridad de la información los riesgos 99, 121 y 124, los cuales, según el control de cambios de los riesgos de procesos, han pasado a ser administrados por la OI DT.

Se identificó un riesgo de Control Interno C01-R4, el cual, por sus características, corresponde a la matriz de riesgos de seguridad de la información y no a un riesgo de proceso.

6. RECOMENDACIONES

La Oficina de Control Interno del INM dada la naturaleza iterativa de la administración de riesgos que implica revisar y ajustar constantemente las estrategias y acciones en función de la evolución de los riesgos y las circunstancias cambiantes de la organización y que permite una mayor adaptabilidad y flexibilidad en la gestión de riesgos, ya que permite responder de manera efectiva a nuevos riesgos, cambios en el entorno empresarial o retroalimentación de los resultados de las acciones tomadas, sugiere que:

- ✚ Continuar fortaleciendo el conocimiento de los funcionarios del INM en la identificación y metodología de gestión de riesgos dentro de los procesos, específicamente, enfocarse en identificar eventos que puedan desencadenar su materialización, lo que promoverá el autocontrol y un seguimiento periódico por parte de los responsables (primera línea).
- ✚ Proseguir con el proceso de identificación de riesgos para permitir que la entidad reaccione oportunamente ante cualquier evento.
- ✚ Realizar ajustes en las matrices de riesgos y en el Isolucion para reflejar información real y congruente entre los diferentes sistemas de información.
- ✚ Consultar las observaciones en materia de riesgos realizadas por la OCI, tanto en los informes de riesgos como en las auditorías de la vigencia 2023 y el seguimiento a la estrategia anticorrupción de la presente vigencia.
- ✚ Atender los lineamientos definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas que estén vigentes, así como cualquier otro reglamento interno o externo que los rija
- ✚ Para la segunda línea, se recomienda que se tenga enfoque de auditoría de riesgos de fraude, es decir, evaluar la efectividad de los controles internos establecidos para prevenir y detectar actividades fraudulentas. Esto incluye revisar políticas, procedimientos y sistemas de monitoreo para identificar posibles brechas que puedan ser explotadas por perpetradores de fraude, así como analizar los procesos de reporte y comunicación de irregularidades para garantizar una denuncia clara de actividades sospechosas y la adopción de medidas correctivas oportunas.
- ✚ Se deben analizar los resultados de auditorías, e informes a entes de control y realizar investigaciones detalladas para identificar posibles áreas de mejora y recomendar acciones correctivas para mitigar los riesgos de fraude identificados.

7. ANEXOS

Ninguno.

Sandra Lucía López Pedreros
Jefe de Oficina de Control Interno
2024-06-02