

	INFORME DE AUDITORÍA DE CONTROL INTERNO	Código: C1-01-F-006
		Versión: 01
		Página 1 de 49

INFORME DEFINITIVO

FECHA DE EMISIÓN DEL INFORME:	11-12-2023
MACROPROCESO:	N/A
PROCESO:	Gestión de las Tecnologías de la Información - (E-05)
LÍDER DEL PROCESO:	Rodolfo Manuel Gómez Martínez Jefe Oficina de Informática y Desarrollo Tecnológico
OBJETIVO(S) DE LA AUDITORÍA:	Verificar el cumplimiento de la evaluación de la gestión de tecnologías de la información de manera que se esté fortaleciendo la parte estratégica de la entidad, de acuerdo con una muestra en la medición y análisis de los indicadores del proceso
ALCANCE DE LA AUDITORÍA:	Información del 01-01-2023 al 30-09-2023

METODOLOGÍA Y / O FICHA TÉCNICA

A continuación, se detallan los aspectos y características que se tuvieron en cuenta para el desarrollo de la auditoria y la preparación del informe:

- 1. Plan de auditoría:** Fue enviado a los involucrados mediante correo electrónico el 09/11/2023 a las 15:54 y posteriormente reiterado durante la reunión de apertura, llevada a cabo vía Teams el 2023-11-14 a las 9:00. El 13 de noviembre se recibió un correo del jefe de la Oficina de Informática y Desarrollo Tecnológico (OIDT), solicitando su reprogramación para las 14:30 del mismo día.
- 2. Reunión de apertura:** La auditoría se inició formalmente el 14 de noviembre de 2023 en una sesión virtual, con la presencia de la Oficina de Informática y Desarrollo Tecnológico (OIDT) representada por: a) Rodolfo Manuel Gómez Martínez - Jefe de la Oficina; b) Alexandra Hernández Moreno – Contratista; c) Alba Graciela Rodríguez Rincón – Contratista; d) Jhon Alexander Torres Galindo – Profesional Especializado; e) Martha Lucia Forero Bermúdez - Contratista; f) Liliana Pineda Aponte – Contratista. Además, se contó con la asistencia de la Oficina de Control Interno, representada por: a) Sandra Lucía López Pedreros - Jefe de la Oficina; b) Johana Andrea Ávila Caballero – Profesional, y c) Ana Yancy Urbano – Contratista.
- 3. Carta de Representación:** Enviada vía correo electrónico el 09/11/2023, junto con la carta de alcance y el plan de auditoría, devuelta firmada el 14/11/2023.

4. Procedimientos de auditoría: Para efectos de llevar a cabo la auditoria se tuvieron en cuenta entre otros los siguientes:

Consulta: Se realizó indagación a través de preguntas orales y escritas, al personal asignado para esta atender esta auditoría.

Rastreo: Se realizó una verificación de la información, para constatar la integridad de la información documentada o registrada.

Confirmación: Se realizó consulta a páginas externas, respecto a temas específicos para el desarrollo de la auditoria que serán incorporados en el resultado.

Se realizó solicitud de información al área auditada, a través de correo electrónico de fecha 15/11/2023:

- Ficha de inversión del proyecto de Oficina de Tecnologías, avance de los indicadores del proyecto de inversión de esta vigencia y su respectivo seguimiento de los resultados ya ejecutados.;
- Avances y evidencias de lo planeado y ejecutado en el Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI;
- Avances y evidencias de lo planeado y ejecutado en el Plan Operativo de Seguridad – POSI;
- Evidencias de la aplicación-ejecución de los controles de los riesgos, definidos por el proceso, así como el resultado del monitoreo y evaluación realizados desde la primera línea de defensa, y reporte a la Oficina Asesora de Planeación -OAP.
- Matriz de activos de información.
- Indicadores del proceso, la evidencia de avance y resultados obtenidos.

5. Fuentes de Consulta e información: consideradas como criterio y/o como medio de validación durante la ejecución de la auditoría.

- ✓ Caracterización del proceso.
- ✓ Página web (www.inm.gov.co)
- ✓ INMtranet
- ✓ Portal SPI_DPN (<https://spi.dnp.gov.co/Consultas/Default.aspx>); en calidad de usuario anónimo
- ✓ Isolución
- ✓ Matriz Riesgos, Aprobación CIGD 10-2023
- ✓ Sistema de Seguimiento de Planes de Mejoramiento – SISEPM

RESUMEN EJECUTIVO

Proyecto de Inversión

Se lleva a cabo una revisión en la página web del Departamento Nacional de Planeación (DNP), específicamente en la ficha del proyecto de inversión:

FICHA EBI
SISTEMA UNIFICADO DE INVERSIONES Y FINANZAS PUBLICAS - SUIFF

Código Bpin: 2017011000369
Nombre del Proyecto: INNOVACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN EN EL INSTITUTO DE METROLOGÍA NACIONAL

INFORMACIÓN GENERAL DEL PROYECTO

Horizonte: 2018 - 2025
Sector: Comercio, Industria y Turismo
Entidad Responsable: 350500-INSTITUTO NACIONAL DE METROLOGÍA - INM
Programa: 3599-FORTALECIMIENTO DE LA GESTIÓN Y DIRECCIÓN DEL SECTOR COMERCIO, INDUSTRIA Y TURISMO
SubPrograma: 0200-INTERSUBSECTORIAL INDUSTRIA Y COMERCIO

ESTADO DE LA FICHA **IMAGEN DEL PROYECTO**

Estado	Registrado Actualizado
Usuario Formulator	Luis Gabriel Miele Benavides
Fecha del Estado Actual	2022-12-22 10:12:04
Fecha Control Posterior	2022-12-22 10:12:04
Solicitud de Formulación	045584 - Sin trámites presupuestales
Vigencia Seleccionada	2023
Fecha Creación del Turno	N/A
Turno de trámite	N/A



Imagen pendiente

INFORMACIÓN BÁSICA

Objetivo

Fomentar la construcción de un estado más transparente, participativo y colaborativo

Fuente: Página del DNP

Código Bpin: 2017011000369 **PND:**
Sector: Comercio, Industria y Turismo Fortalecimiento de la gestión y dirección del Sector Comercio, Industria y Turismo
Entidad: Metrología - Inm
Responsable: Luis Gabriel Miele Benavides
Horizonte: 2018 - 2025
Presupuesto 2023: \$3.246.749.536
Control Posterior: 22/12/2022
Seguimiento de: Octubre 2023

[Resumen Ejecutivo](#) [Ficha EBI\(22/12/2022\)](#) **Avance Físico:** :0,00%
Avance Financiero: :35,14%
Avance Gestión: :0,00%

[Cadena de Valor](#) | [Esquema Financiero](#) | [Metas Ind. Secundarios](#) | [Metas de Gestión](#) | [Regionalización](#) | [Anexos](#) | [Beneficiarios](#)

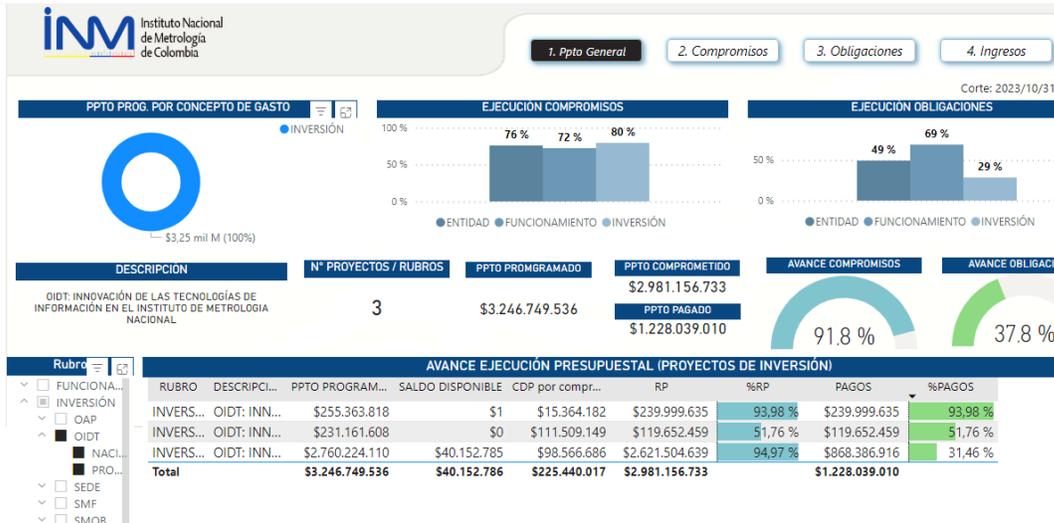
Cifras en Pesos Corrientes

Vigencia	Solicitado**	Inicial*	Vigente*	Compromiso*	Obligación*	Pago*	Avances
2018-Dic	0	990.722.755	966.722.755	849.582.702	773.397.034	628.405.050	Financiero: 80,00% Físico: 94,39% Gestión: 97,60%
2019-Dic	5.246.750.000	1.480.000.000	1.431.670.000	1.218.578.341	678.148.079	670.426.467	Financiero: 47,37% Físico: 63,88% Gestión: 93,80%
2020-Dic	5.588.425.000	2.500.000.000	2.574.612.461	2.273.758.346	1.889.890.681	1.680.915.582	Financiero: 73,40% Físico: 90,64% Gestión: 93,85%
2021-Dic	5.865.667.500	1.953.077.120	1.953.077.120	1.436.926.987	1.436.926.987	1.368.804.675	Financiero: 73,57% Físico: 26,62% Gestión: 167,90%
2022-Dic	5.754.578.980	2.000.000.000	2.000.000.000	1.520.277.950	1.431.233.032	1.431.233.032	Financiero: 71,56% Físico: 19,09% Gestión: 85,45%
2023-Oct	7.283.670.623	3.246.749.536	3.246.749.536	2.676.154.674	1.140.999.661	1.140.999.661	Financiero: 35,14% Físico: 0,00% Gestión: 0,00%
2024	7.522.508.443	0	0	0	0	0	Financiero: 0,00% Físico: 0,00% Gestión: 0,00%

Fuente consulta: DNP

El proceso cuenta con un presupuesto de \$3.246.749.538, correspondiente al presupuesto nacional de \$2.760.224.110 y recursos propios de \$486.525.426. Hasta la fecha, se han comprometido \$2.676.154.674, lo cual ha sido corroborado con la información del micrositio de OAP, disponible en la intranet. A continuación, se detalla el siguiente tablero de control:

 Ejecución Presupuestal



Fuente: https://metrologiainm.sharepoint.com/sites/oap_share/SitePages/presup.aspx?source=https%3A%2F%2Fmetrologiainm.sharepoint.com%2Fsites%2Foap_share%2FSitePages%2FForms%2FByAuthor.aspx

Durante la reunión mantenida con el auditado, se revisaron las cifras correspondientes a lo ejecutado. Se observó que los valores comprometidos están adecuadamente respaldados por contratos en curso, los cuales se están desarrollando para alcanzar las metas establecidas y que son verificados en las auditorías a los procesos de gestión financiera y de adquisición de bienes y servicios.

Resultado revisión del Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI

Se examinó el progreso de cada proyecto y sus actividades, evaluando las evidencias proporcionadas. La programación abarcó desde el mes 4 hasta el mes 12. A continuación, se detalla la revisión llevada a cabo por proyecto y su respectivo estado de avance:

1. PROYECTO: GOBERNANZA E IMPLEMENTAR LA ESTRUCTURA Y PROCESO DE GESTIÓN DE TI / INSTITUCIONALIZAR Y FORTALECER EL EQUIPO ASESOR DE AE DE TI (ID -2 Y ID-7)

Subproyecto **Metrología 4.0 para una transformación digital sostenible de las mediciones y la trazabilidad** el cual contiene dos (2) actividades:

- + **Actividad: Implementación de un esquema de gobernanza y los procesos asociados para la gestión de TI.** Se programaron 3 productos: Primer entregable: a) Un (1) Acta de aprobación de CIGD de los equipos de arquitectura; Segundo entregable; b) Una (1) actualización caracterización

del proceso; c) Tercer entregable: Una (1) Sensibilización sobre el esquema de gobernanza; con fechas de cumplimiento para el mes 5 (2 productos) y mes 6 (un producto); En descripción de ejecución del mes 5, se indica que *"Se Elaboró Manual de Gobierno Digital en el cual se incluyó la conformación de los equipos de arquitectura empresarial, este se envió a OAP para su revisión, se espera aprobación en el próximo CIGD."*

En el periodo se realizó socialización del esquema de gobernanza al equipo de OIDT el 2023-05-31".

Al contrarrestar la información en el aplicativo ISOLUCIÓN - módulo de documentación, a la fecha no se registra el documento antes mencionado; como evidencia se aportó el documento en versión borrador de fecha mayo de 2023. Por lo anterior, se concluye que, aunque los esfuerzos se encuentran concentrados para dar cumplimiento en esta vigencia; la ejecución de los productos no da cuenta del cumplimiento de esta actividad, aunque se registre un avance del 33%.

- ✚ **Actividad: Establecer la arquitectura de TI.** Se programó un (1) documento, el cual tiene como fecha de finalización el mes 12; no se registra avance hasta el mes 6; sin embargo, en los registros de seguimiento se observa que el mes 7 se registra que están identificando las empresas que prestan estos servicios en el mercado para proceder con la contratación y, en el mes 8 se indica que se estructura y radica el proceso de contratación y se identifica el cambio de entregable. Como se evidenció, el acta de inicio del contrato N° 166 de 2023 de fecha 18/10/2023 con el objeto de *"CONTRATAR LOS SERVICIOS PARA AVANZAR EN EL DESARROLLO DE LA POLÍTICA DE GOBIERNO DIGITAL EN EL INSTITUTO NACIONAL DE METROLOGÍA"* para este producto su avance continuo en 0%. Como recomendación, se indica que se verifiquen y se clarifiquen los entregables por parte del contratista para dar el respectivo cumplimiento a lo planeado en el PETI.

Subproyecto **Eficiencia en la operación de TI**, se programaron tres (3) actividades:

- ✚ **Consolidación de la operación bajo una estructura homogénea (Microsoft).** Productos: a) Primer entregable: Diagnóstico; y b) Segundo entregable: Informe de ejecución. Actividades que se registran programadas para el mes de 5 y mes 12 respectivamente. De acuerdo con registro de avance, se indica que se hizo entrega del diagnóstico para la implementación de herramienta de integración Microsoft en el mes 8, se inicia la implementación de migración, en el mes 9 se indica la ejecución o las últimas actividades de migración, con un resultado de avance del 50%. Una vez revisada la evidencia del diagnóstico, se observa que este documento da

cuenta al cumplimiento del producto y este se registra con fecha del 30/05/2023. Para esta actividad se encuentra en proceso el último producto que es el informe de ejecución que se tienen proyectado para el mes de 12.

✚ **Mejoramiento de la seguridad perimetral**, se programaron dos (2) productos: a) Primer entregable: Diagnóstico y b) Segundo entregable: Informe de ejecución, con programación respectivamente para el mes 7 y 12. Como evidencia, se observa el documento "*Diagnostico mejoramiento de la seguridad perimetral*" de fecha 01/08/2023 con contenido en ocho (8) paginas, adicional se aporta el clausulado del contrato N°148 de 2023, permitiendo evidenciar la adquisición de elementos para la seguridad perimetral como lo es servidor de backup y el respectivo software. Sin embargo, dando lectura al documento diagnóstico, no se observa que se defina la línea base de cómo está la entidad en esta materia, y cuál es la proyección en materia de adquisición de productos o servicios; adicional no se detalla cómo está construida la red de datos de la entidad y que mejoras se van a aplicar en los diferentes niveles de seguridad. Esto puede ocasionar, sobredimensionar la necesidad y adquirir soluciones que no estén acordes. Se recomienda, que en la estructuración de documentos técnicos contemplen tanto la proyección de inversión como la descripción de beneficios a generar.

✚ **Mejoramiento de la capacidad de procesamiento (servidores)**, contiene dos (2) productos: a) Primer entregable: Diagnóstico, y b) Segundo entregable: Informe de ejecución con fechas de cumplimiento para el mes 6 y 11 respectivamente, se registra un avance del 100%. Se revisa evidencia: remisión de entregas de equipos y Licencias emitido por el proveedor *Realtime Consulting & Services* de fecha 30/10/2023 y Acta de inicio de contrato N° 148-2023, sobre la adquisición de una solución de Backups, respaldo de información y servidores para actualizar la infraestructura tecnológica del INM, y documento de Clausulado Contrato N°148-2023 donde se indican las diferentes obligaciones y elementos adquiridos para el tema de backups, producto que dio cumplimiento.

2. PROYECTO: **SERVICIOS DIGITALES METROLOGÍA/ GOBIERNO DE DATO: FUENTE ÚNICA DE INFORMACIÓN DE METROLOGÍA / AUTOMATIZACION DE SERVICIOS (FASE I Y II) FASE I: AUTOMATIZACION DE 5 SERVICIOS (100%) Y FASE II: EXPONER ANTE GOV.CO (ID 1, ID-4M ID-8)**

• **Subproyecto: Integración de Servicios ciudadanos Digitales con gov.co**

Para este subproyecto se definieron tres (3) productos:

✚ **Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co para hora legal**, como producto se definió: Matriz de cumplimiento de los estándares de usabilidad y accesibilidad web, con fecha de cumplimiento en el mes 5. Registrando un avance del 100%, revisada la evidencia "6. *Matriz Hora Legal junio 2023*", se observa el respectivo cumplimiento.

✚ **Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co para página web**, como producto se definió: Matriz de cumplimiento de los estándares de usabilidad y accesibilidad web, con fecha de cumplimiento en el mes 5. Una vez revisada la evidencia "7. *Matriz página web.xlsx*", con un avance del 100%; sin embargo, al revisar el archivo se observó que desde la línea 109 a la 255 no se encuentra diligenciada, lo que no permite ver la debida evaluación que debe efectuar la oficina de OI DT frente a este requerimiento.

✚ **Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co de los servicios ofrecidos por la entidad**, tiene definido el producto Matriz de cumplimiento de los estándares de usabilidad y accesibilidad web, este se tiene programado para el mes 11; sin embargo, sólo hasta el mes 7 y 8 se registra un avance, mientras en el mes 9 se registra "Por parte de OI DT se solicitará cambio de la actividad por: *Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co para un servicio ofrecido por la entidad, atendiendo a que se depende del otras instancias para dar cumplimiento a los cinco servicios*", indagando con los auditados, se menciona que este cambio no se ha presentado ante el Comité de Gestión y Desempeño. Por lo anterior, se recomienda tomar las medidas pertinentes con el fin de no incumplir con esta actividad y así no afectar el cumplimiento del PETI de la vigencia.

3. Proyecto: **GESTIÓN DOCUMENTAL FASE I (100%) / GESTIÓN DOCUMENTAL FASE II / GOBIERNO DE DATO: FUENTE ÚNICA DE INFORMACIÓN DE METROLOGÍA (ID-9 Y ID-4)**

✚ **Subproyecto: Gestión de la Información**

Para este subproyecto se definieron 3 productos así:

✚ **Solución de Back Up para preservación de la información**, como productos se definieron: a) Primer entregable: Diagnóstico, y b) Segundo entregable: Informe de ejecución con fechas de cumplimiento mes 5 y mes 11 y su avance corresponde al 50%. Verificada la evidencia se observó: el archivo "9. *DIAGNOSTICO SOLUCION BACKUP.pdf*", evidenciando de manera detallada la necesidad que tiene el instituto frente a este tema, adicional en registro del mes 8, se indica que ya se adjudicó el contrato N°148-2023, el

cual provee la solución de backup y se encuentra al pendiente el producto para el mes de 11 y así completar la meta.

✚ **Fortalecimiento de la capacidad operativa** como productos se definieron: a) Primer entregable: Diagnóstico, y b) Segundo entregable: Informe de ejecución con fechas de cumplimiento mes 5 y mes 11, su avance corresponde al 50%. Verificada la evidencia se revisó: documento "10. Concepto diagnostico estado elementos equipos (1).pdf", el cual describe el nivel de obsolescencia de los equipos de cómputo y porque se deben renovar. En el registro del seguimiento para el mes 9, se indica que se adjudicaron las órdenes de compra 116270 y 116268 que se destinaron para la adquisición de equipos de cómputo.

✚ **Fortalecimiento de los sistemas de información**, como productos se definieron: a) Primer entregable: Un (1) inventario de soluciones; b) Segundo entregable: Un (1) Informe de avance de implementación de soluciones; y c) informe final de implementación de soluciones, con fechas de cumplimiento en los meses de 6,9 y 12, se registra un avance del 67%. Verificada la evidencia se observó archivo "11. E-05-F-033CATLOGOSISTEMASDEINFORMACININM (2).xlsx", el cual describe el inventario de los sistemas de información y software de gestión de la Entidad; y archivo "11. E02F011ModeloInformeV.4m (3) (1).pdf" del mes de junio de 2023, documento que describe el diagnóstico de la capacidad de procesamiento, siendo este un proceso esencial para evaluar la eficiencia y el rendimiento de los recursos informáticos en el Instituto Nacional de Metrología; sin embargo, este no contempla las características que deben tener los nuevos servidores que requiere la entidad para soportar la operación; en cuanto al informe de avance de implementación no se tiene que es el producto del mes 9.

4. Proyecto: **FORTALECER EL SISTEMA DE GESTIÓN, CONTROL Y SEGUIMIENTO ADMINISTRATIVO / AUTOMATIZACION DE SERVICIOS (FASE I Y II), FASE I: AUTOMATIZACION DE 5 SERVICIOS (100%), FASE II: EXPONER ANTE GOV.CO (ID-6, ID-8 y ID-11) -FASE I: TRANSICIÓN IPV4 IPV6 (100%), FASE II: TRANSICIÓN IPV4 IPV6 (100%), FASE III: TRANSICIÓN IPV4 IPV6 (100%), FASE IV: TRANSICIÓN IPV4 IPV6.**

✚ Subproyecto: **Seguridad Digital - actualización de la 27001:2022**,

Para este subproyecto se definieron 3 productos así:

✚ **Diagnóstico de la arquitectura frente a la seguridad digital**, como

productos se definieron: a) Primer entregable: Un (1) Autodiagnóstico MSPI y, b) Segundo entregable: Un (1) Autodiagnóstico Seguridad Digital, con fechas de cumplimiento en los meses de 5 y 6, su avance se registra en el 100%. Verificada la evidencia se observó: el archivo "14. MSPI INM marzo2023.xlsx", el cual permite evidenciar el estado de la entidad en esta materia; sin embargo, en la pestaña de Portada, se detalla la información es para la vigencia 2020, como se evidencia en la siguiente imagen:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	26%	40%
	Implementación	11%	20%
	Evaluación de desempeño	12%	20%
	Mejora continua	14%	20%
TOTAL		63%	100%

Fuente: pestaña Portada del archivo "MSPI INM marzo2023.xlsx"

Por otra parte, se recomienda diligenciar la información en todas las pestañas, dado que en las pestañas "Levantamiento de Info." y "Áreas Involucradas" no se encuentran diligenciadas. Lo anterior, con el fin de tener clara las necesidades y las responsabilidades. Ahora bien, frente al Archivo "12. Diagnostico ISO27001 2022 INM rev Oct23.xlsx", que corresponde al producto N° 2 se detalla por control que aplica la entidad. Se recomienda, que frente a lo que se encuentra pendiente o falta por fortalecer, se establezca un cronograma de actividades para que se alcance la meta y sea medible.

✚ **Hoja de ruta de implementación de seguridad Digital**, como producto se definió "Hoja de ruta de implementación de seguridad Digital", con fecha de cumplimiento en el mes 7, su avance se registra en el 100%; se aportó como evidencia archivo "13 y 14 Hoja de Ruta Seguridad Digital.xlsx", este contiene seis (6) actividades que se encuentran programadas dentro de los meses 7 al 12, se observa el que se está realizando el seguimiento.

✚ **Seguimiento de implementación de la hoja de ruta de seguridad digital**, como producto se definió Dos (2) Informes de seguimiento, con fecha de cumplimiento en el mes 9 y 12, su avance se registra en el 50%. Se aportó como evidencia el archivo "13y 14 Hoja de Ruta Seguridad Digital.xlsx", en este se puede observar el avance, pero no tiene el objetivo de ser informe, por lo que se sugiere mejorar la construcción de las evidencias.

Resultado revisión del Plan Operativo de Seguridad – POSI

Este plan contempla 7 actividades las cuales se encuentran en porcentaje de avance del plan total con un 73,9%, distribuido así:

No. ÍTEM	ACTIVIDAD	PRODUCTO / ENTREGABLE	META ANUAL	AVANCE ANUAL	% DE AVANCE
1	Fase diagnóstica: Revisión de información existente, establecer estado actual de implementación de SGSI y MSPI	Documento Evaluación SGSI ISO27001:2022 y MSPI	1	1	100%
2	Fase de Planeación: Establecer plan y cronograma de seguridad y privacidad 2023	Documento	1	1	100%
3	Fase de implementación: Actualizar matriz de activos	Matriz de activos en ISOLUCION	1	1	100%
4	Fase de implementación: Actualizar procedimientos de seguridad y manual de políticas seguridad, según resultado del diagnóstico.	Procedimientos de controles de seguridad y manual de políticas de seguridad de la información actualizados	23	20	87%
5	Evaluación y desempeño: Gestionar el cierre de hallazgos asociados a seguridad de la información (17 hallazgos abiertos en ISOLUCION)	Hallazgos cerrados en ISOLUCION	17	12	71%
6	Revisar informes de análisis de vulnerabilidades y Contratar servicios para definir y ejecutar análisis de vulnerabilidad 2023 a sistemas críticos y realizar remediaciones	Documento con vulnerabilidades y documento de seguimiento a remediaciones	1	0	0%
7	Hacer capacitaciones de concientización en seguridad de la información: boletines y charlas	Material de capacitación	5	3	60%

Fuente: Archivo POSI Seguridad y Privacidad de la Inf de la OIDT

A continuación, se relaciona la revisión efectuada por actividad y su respectivo avance:

- 1. Fase diagnóstica: Revisión de información existente, establecer estado actual de implementación de SGSI y MSPI**, como producto se definió el Documento Evaluación SGSI ISO27001:2022 y MSPI, con fecha de cumplimiento el mes 4, registrando el avance del 100%. Una vez revisada la evidencia se observó que se cuenta con archivos de: "*Diagnostico ISO27001 2022 INM.xlsx*" y "*Diagnostico ISO27001 2022 INM rev Oct23.xlsx*", adicional el archivo de MSPI que se presentó para PETI, lo cual permite evidenciar que se dio cumplimiento a los productos.
- 2. Fase de Planeación: Establecer plan y cronograma de seguridad y**

privacidad 2023, como producto se definió Documento, con fecha de cumplimiento el mes 3, registrando el avance del 100%. Una vez revisado el registro de seguimiento, se indica que “[...]Se elabora plan de seguridad y privacidad de la información y plan de tratamiento de riesgos de seguridad de la información para el año 2023. Se presentan y aprueban en CIGD N° 5 del 2023-03-29 y 2023-04-04[...]”; se revisa actas y se observó que se trató el tema el 23 de marzo y 4 de abril.

3. Fase de implementación: Actualizar matriz de activos, como producto se definió: “Matriz de activos en isolucion”, con fecha de cumplimiento el mes 5, registrando el avance del 100%. Una vez revisada la evidencia “1.7. E-05-F-005-Inventario-AI-v2.1-2023.xlsx” se observa en Isolución la versión 2

Fecha de actualización				YYYY/MM/DD					Código: E-05-F-005	
Fecha de actualización				YYYY/MM/DD					Versión: 2	
Fecha de actualización				YYYY/MM/DD					Página: Ver pie de Pág	
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN										
Activo	AREA	PROCESO	NOMBRE O CATEGORIA DEL ACTIVO	Clasificación o reserva total o parcial de la información	Fecha de calificación	Frecuencia de actualización	Categoría lugares de consulta	Detalle Lugar de Consulta		
	Seleccione área	Diligencie el proceso al que pertenece el activo según el mapa de procesos de la entidad	Nombre que lo identifique de manera precisa y a través del cual se identificará el activo de información.	Seleccione como se debe aplicar la reserva sobre la información del activo	Registre la fecha yyyy-mm-dd en la cual se realiza la clasificación de la información como reservada o clasificada	Seleccione la periodicidad o el segmento de tiempo bajo el cual actualiza la información, de acuerdo a su naturaleza o a la normativa aplicable	Seleccione donde a través de que mecanismo se puede consultar la información	Registre URL, Nombres de aplicativos, lugares físicos, etc. asociados al lugar de consulta.		

Fuente: imagen de archivo generado en ISOLUCIÓN

Y el archivo suministrado se encuentra en la versión 1.8,

Fecha de actualización				2023-05-23					Código: E-05-F-005			
Fecha de actualización				2023-05-23					Versión: 18			
Fecha de actualización				2023-05-23					Página: Ver pie de Pág			
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN												
Activo	AREA	PROCESO	PROCEDIMIENTO	NOMBRE O CATEGORIA DEL ACTIVO	Descripción de condición legítima de excepción	Clasificación del activo de acuerdo con transparent ley 1712	Plazo de Clasificación Reserva	Clasificación o reserva total o parcial de la información	Fecha de calificación	Frecuencia de actualización	Categoría lugares de consult	Detalle Lugar de Consulta
Activos de tipo "Datos / Información" y "Bases de datos"												

Fuente: Imagen de archivo 1.7. E-05-F-005-Inventario-AI-v2.1-2023.xlsx

Este archivo se encuentra estructurado por pestaña y en cada una se definen los activos de información de cada proceso; sin embargo, se recomienda actualizar la versión del documento.

4. Fase de implementación: Actualizar procedimientos de seguridad y manual de políticas seguridad, según resultado del diagnóstico, como producto se definió “Procedimientos de controles de seguridad y manual de políticas de seguridad de la información actualizados”, con registro de avance del 87% y su programación es:

PROGRAMACIÓN											
M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
		1	2	4	3	4	3	3	2	1	

Fuente: Matriz POSI Seguridad y Privacidad de la Información

Es decir que para el mes 9 se deben tener 20 documentos, y se procede con la revisión de los registros de seguimiento así:

- ✚ **M3:** se registra que se “[...]Se elaboró el procedimiento E-05-P-00XX ADQUISICIÓN, ADMINISTRACIÓN Y CONTROL DE USO DE LICENCIAS DE SOFTWARE con sus respectivos formatos: E-05-F-00XX Solicitud de Software licenciado y o renovación, E-05-F-00XX Inventario y Control de software licenciado, Acuerdo Confidencialidad. [...]”; sin embargo, al verificar en Isolución se observó que el documento, el primer documento fue aprobado el 30/04/2023 y los formatos no se evidencian, por lo que se incumple para este mes con la meta.
- ✚ **M4:** se registra: “[...]Se aprobó el procedimiento E-05-P-012 ADQUISICIÓN, ADMINISTRACIÓN Y CONTROL DE USO DE LICENCIAS DE SOFTWARE, y formato: E-05-F-032 Compromiso de Buen Uso de las Licencias de Software[...]”, se revisa las fechas de aprobación en Isolución del 30/04/2023 y 28/04/2023 respectivamente. Lo que permite ver el cumplimiento de la meta.
- ✚ **M5:** se registra: “Se actualizaron y aprobaron en Isolución los siguientes documentos incluyendo controles de Seguridad de la Información:
 - E-05-P-008 Gestión de incidentes de Seguridad de la Información, se aprobó el 31/05/2023 actualmente registra otra actualización el 31/10/2023
 - E-05-P-003 Gestión de Incidentes y Requerimientos de Servicios de TI, con fecha de aprobación del 31/05/2023
 - Se elaboró el Manual de Gobierno Digital y se envió a OAP para revisión; aún no se registra en Isolución
 - Actualizó el Manual de Seguridad de la Información y se envió a OAP para revisión, se registra con fecha 21/07/2023.”; en revisión en Isolución y sólo se cumplió con 2 (E-05-P-008 y E-05-P-003) de los 4 documentos programados.
- ✚ **M6:** se registra: “Se actualizaron y aprobaron en isolucion los siguientes documentos incluyendo controles de Seguridad de la Información:
 - E-05-P-013 Procedimiento adquisición, desarrollo y mantenimiento de software y automatización de mediciones en V1
 - E-05-I-010 Configuración de Recursos Compartidos en V3
 - E-05-D-004 Infraestructura Tecnológica y Redes”; en revisión se observa que los documentos tienen fecha de aprobación del 30/06/2023 (E-05-P-013

y E-05-I-010) y 01/07/2023 para el documento E-05-D-004. Lo anterior, permite evidenciar el cumplimiento parcial de los productos.

- ✚ **M7:** se registra: “Se actualizaron y aprobaron en isolucion los siguientes documentos incluyendo controles de Seguridad de la Información:
- E-05-P-011 Procedimiento Control De Acceso A Los Servicios Tecnológicos Y Sistemas De Información Del INM.
- E-05-P-014 Generación, Administración y Restauración de Copias de Respaldo de la información
- E-05-I-023 Apagado y Encendido de la Infraestructura de TI
- E-05-I-024 Etiquetado de Información”; al revisar en Isolución se observó que las fechas de publicación son el 13/07/2023 (E-05-P-014), 26/07/2023 (E-05-I-023) y 31/07/2023 (E-05-P-011 y E-05-I-024). Lo que permite evidenciar el cumplimiento de la meta.

- ✚ **M8:** se registra: “Se actualizaron y aprobaron en isolucion los siguientes documentos incluyendo controles de Seguridad de la Información:
- E-05-P-015 Creación y Deshabilitación de Usuario del Directorio Activo
- E-05-I-014 Configuración de Perfil de Usuario
- Propuesta de controles de seguridad de la información enviada a Secretaria General (enlace de calidad) para actualización de documentación de talento humano y adquisición de bienes y servicios.”; al verificar en Isolución se encuentran con fecha 31/08/2023 (E-05-P-015 y E-05-I-014), Lo anterior, permite evidenciar el cumplimiento parcial de los documentos.

- ✚ **M9:** se registra: “Se actualizaron y aprobaron en isolucion los siguientes documentos incluyendo controles de Seguridad de la Información:
- E-05-P-016 Mantenimiento de la infraestructura Tecnológica.
- E-05-I-025 Autenticación de Múltiples Factores (MFA) en Office 365
- E-05-P-017 Gestión de Vulnerabilidades de TI”; sin embargo, al revisar en Isolución se registran con fecha 21/09/2023 (E-05-I-025), 27/09/2023 (E-05-P-016) y 28/09/2023 (E-05-P-017). Lo que permite evidenciar el cumplimiento de los productos.

Como conclusión general, se observa que no se ha dado cumplimiento en 4 documentos, tal y como se observó en el mes 3, 4 y 8; se sugiere que estos sean cumplidos antes de finalizar la vigencia.

5. Evaluación y desempeño: Gestionar el cierre de hallazgos asociados a seguridad de la información (17 hallazgos abiertos en Isolución), como producto se definió “*Hallazgos cerrados en Isolucion*”, con la siguiente programación en ejecución y registro de avance del 71%:

PROGRAMACIÓN												META ANUAL
M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	
			1	2	2	2	2	2	2	2	2	17

Fuente: Matriz POSI Seguridad y Privacidad de la Información

✚ **M4:** Se registra el seguimiento "Se realizó gestión de cierre del hallazgo Acción Correctiva AUD #51 mediante correo del 27 de abril ante OAP, este fue cerrado por dicha oficina posteriormente en Isolución. Se adjunta correo y pantallazos."; se observa en Isolución el respectivo cierre con soporte respectivo.

✚ **M5:** Se registra el seguimiento "Se realizó cierre de dos hallazgos: Acción correctiva AUD 56, Observación AUD #138 mediante correo del 30 de mayo la OAP aprueba cierre en Isolución. Se adjunta correo". Se observa en Isolución el respectivo cierre con soporte.

✚ **M6:** Se registra el seguimiento "Se realizó cierre de los siguientes hallazgos de seguridad de la información:
- Isolución: Observación AUD #141
- Contraloría: Código de Hallazgo 26."

Se observa en Isolución el respectivo cierre con soporte.

✚ **M7:** Se registra el seguimiento "Se realizó cierre de los siguientes hallazgos de seguridad de la información:
- Acción Correctiva AUD #46
- Acción Correctiva AUD #135
- Acción Correctiva AUD #134"

Se observa en Isolución el respectivo cierre con soporte.

✚ **M8:** Se registra el seguimiento: "Se realizó cierre de los siguientes hallazgos de seguridad de la información:
- Acción Correctiva 34
- Observación AUD #142
- Observación AUD #143"

Se observa en Isolución el respectivo cierre con soporte.

✚ **M9:** Se registra el seguimiento: "Se realizó cierre de los siguientes hallazgos de seguridad de la información:
- Acción Correctiva AUD #13
- Acción Correctiva AUD #17"

- Observación AUD #221"

Se observa en ISOLUCIÓN el respectivo cierre con soporte.

6. Revisar informes de análisis de vulnerabilidades y Contratar servicios para definir y ejecutar análisis de vulnerabilidad 2023 a sistemas críticos y realizar remediaciones; como producto se definió "Documento con vulnerabilidades y documento de seguimiento a remediaciones", programado en ejecución para el mes 10, con registro de avance del 0%; sin embargo, en avances se indica sólo se registra avance para el mes 9, indicando "*Se radica proceso de Ethical Hacking en contratos, por medio del cual se identificarán las vulnerabilidades de la infraestructura de TI a partir de pruebas controladas.* Por lo anterior, se espera que este producto refleje posteriormente el debido cumplimiento al objetivo trazado.

7. Hacer capacitaciones de concientización en seguridad de la información: boletines y charlas, como producto se definió "Material de capacitación" y se registra un avance del 60%, con programación de ejecución así:

PROGRAMACIÓN											
M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
			1		1		1		1		1

Fuente: Matriz POSI Seguridad y Privacidad de la Información

Se aporta como evidencia:

- **M4:** como seguimiento se registra: "*Se realizó capacitación del procedimiento de Gestión de Activos de información (E-05-P-004) a todo el personal del INM los días 24 y 27 de abril, con el objetivo de dar inicio a la actualización de la matriz de activos. Se tienen listados de asistencia*". Como evidencia se aporta:

✚ "Capacitación Gestión de activos de información - *listado.xlsx*"— listado de asistencia con registro de 17 asistentes, de fecha 24/04/2023. No se aporta listado de asistencia del 27 de abril.

- **M6:** como seguimiento se registra: "*Se gestionó la publicación de dos boletines con temas de alerta ante correos electrónicos sospechosos y de Reporta incidentes de seguridad.*", como evidencia se aportó:

✚ Archivo "*Correo - alerta ante correos electrónicos sospechosos!.pdf 2*",

correo electrónico de fecha 27/06/2023 con mensaje de ¡Cuidado con los correos electrónicos sospechosos!.

- ✚ Archivo "*Correo Reporta incidentes de seguridad!.pdf*", correo electrónico del 26/06/2023 con asunto de *iReporta incidentes de seguridad!*.

- **M8:** Se registra como avance: "*Se gestionó la publicación de un boletín con tips para la creación de contraseñas seguras.*", como evidencia se aporta:

- ✚ Archivo: "*boletín seguridad contraseñas seguras.PNG*" – imagen de boletín y no describe cuando se publicó.
- ✚ Archivo: "*Presentación etiquetado activos ago23.pptx*"—presentación del mes de agosto de 2023, sobre el etiquetado de activos de información con contenido de siete (7) diapositivas.

- ✚ **M9:** Se registra como avance: "*Se realizó socialización del procedimiento E-05-P-011 Control de accesos a Servicios de TI.*", no se aporta evidencia.

Otros archivos presentados como evidencias:

- ✚ *1.6.131.3 Políticas de seguridad de la información INM OI.DT.pptx*: presentación con fecha del 27/07/2023, con contenido de 25 diapositivas.
- ✚ *ASISTENCIA - Capacitación - Seg inf oct.xlsx* – listado de asistencia del 26/10/2023, con 76 asistentes, sin embargo, este documento no permite evidenciar que tema fue tratado en esa reunión.
- ✚ *Boletín de seguridad sept.pdf* –se observa que fue publicado el pasado 29/09/2023, el cual se titula como "*¡Ayúdanos a prevenir un ataque informático!*"
- ✚ *Capacitación Gestión incidentes de seguridad de la información.pptx* – presentación con 14 diapositivas (este archivo no indica fecha)
- ✚ *Capacitación políticas de seg INM en redes sociales.pptx*—presentación con seis (6) diapositivas, no se cuenta con la fecha de elaboración.
- ✚ *Sensibilización Seg inf INM oct.pptx*- presentación de 26/10/2023m con el tema de "*Vivamos la Seguridad de la Información en el INM*", con contenido de 24 diapositivas.
- ✚ *Sesión capacitación políticas de seguridad.pdf* – pantallazo de reunión de fecha del 31/10/2023 con asistencia de 11 personas.

Se observó que se han efectuado más actividades de las programadas; sin embargo, es importante que se fortalezca la construcción de las evidencias con el fin, que estas permitan ser identificadas con la fecha de aplicación o elaboración; de igual manera, se recomienda que las actividades que tengan inmersa alguna capacitación efectúen alguna evaluación que permita evidenciar el impacto y grado de apropiación.

Riesgos del proceso

El proceso cuenta con 16 riesgos, descritos a continuación:

✚ Tipo(s) de riesgo(s) de Confidencialidad – tres (3) riesgos

Referencia	RIESGO	CONTROL	Periodo: Cuatrimestre Q1 2023	Periodo: Cuatrimestre Q2 2023	OBSERVACIONES OCI
			Descripción del Avance, Evidencia y/o Observaciones	Descripción del Avance, Evidencia y/o Observaciones	
123	Posibilidad de afectación reputacional por acceso de personal no autorizado a sistemas de información, servicios tecnológicos e infraestructura tecnológica del INM debido al uso incorrecto por parte de los usuarios de las credenciales asignadas por la entidad y por Phishing (Suplantación)	El Profesional de Seguridad de la información concientiza a los usuarios en el uso adecuado de las credenciales asignadas por el INM, con el fin de mitigar fallas en seguridad de la información La OIDT cuenta con el procedimiento Administración de Usuarios para Servicios y Sistemas de información (E-05-002) donde se establecen los Controles de Acceso a la Información	1. Se implementan los Controles de Acceso a la Información con el formato E-05-F-003 Reporte de Novedades de Usuario para Sistemas de Información y Servicios Tecnológicos a través de mesa de servicio. En el periodo no se identificó acceso a la información de usuarios no autorizados. 2. Se actualiza el plan operativo de seguridad y privacidad de la información mediante CIGD N° 5 del 2023-03-29 y 2023-04-04, en el cual se establecen actividades de sensibilización.	En el periodo se ejecutaron las siguientes actividades relacionadas con los controles: 1. Se actualizó el procedimiento E-05-P-011 Procedimiento Control De Acceso A Los Servicios Tecnológicos Y Sistemas De Información Del INM, se direccionó la recepción de solicitudes de accesos por medio de GLPI. En el periodo no se identificó acceso a la información de usuarios no autorizados. 2. Se realizó sensibilización a través de medios sobre contraseñas, así como socialización en el mes de julio sobre las políticas de seguridad de la información.	Las evidencias aportadas dejan observar que se han venido realizando esfuerzos con el fin de revisar el riesgo; sin embargo, es importante que se construyan evidencias que permitan demostrar la aplicación del control; no obstante, el término de "concientiza" en la descripción del control, es ambiguo y no permite evidenciar la eficacia y efectividad que requiere el control.

129	Posibilidad de afectación reputacional por atención de requerimientos de TI y habilitación de roles de acceso a la información por fuera del perfil del usuario debido al poco control sobre las directrices descritas en los procedimientos, instructivos y/o guías establecidas en el proceso de TI	<p>El profesional de Seguridad de la Información define e implementa políticas para la seguridad de la información y la documentación asociada a los controles de acceso con el fin de habilitar los roles de acceso dentro del perfil de usuario a través de las políticas de seguridad de la información y el protocolo respectivo</p> <p>La OI DT cuenta con el procedimiento Administración de Usuarios para Servicios y Sistemas de información (E-05-002) donde se establece el proceso a seguir para la habilitación de roles de acceso a la información</p>	<p>1. Se implementan los Controles de Acceso a la Información con el formato E-05-F-003 Reporte de Novedades de Usuario para Sistemas de Información y Servicios Tecnológicos a través de mesa de servicio. En el periodo no se identificó acceso a la información de usuarios no autorizados.</p> <p>2. Se actualiza el plan operativo de seguridad y privacidad de la información mediante CIGD N° 5 del 2023-03-29 y 2023-04-04, en el cual se establecen actividades de sensibilización.</p>	<p>1. Se realizó actualización del procedimiento E-05-P-011 Procedimiento De Acceso A Los Servicios Tecnológicos Y Sistemas De Información Del INM, y se creó el procedimiento E-05-P-015 Creación y Deshabilitación de Usuario del Directorio Activo.</p> <p>2. No se evidencio desde mesa de servicio la autorización de accesos no autorizados a usuarios, se dio cumplimiento al procedimiento de incidentes y requerimientos. Se tienen ticket de casos generados en GLPI.</p>	<p>Las evidencias aportadas dan cuenta de las actividades adicionales realizadas. Sin embargo, es importante que se construyan evidencias que permitan demostrar la aplicación del control.</p> <p>Ahora bien, si el profesional de seguridad define e implementa políticas, se sugiere asignar a un profesional diferente el seguimiento y monitoreo de los accesos a los aplicativos, con el fin de no concentrar las responsabilidades.</p>
133	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	Cuando ingresa personal a la entidad, el supervisor del contrato, jefe de oficina o subdirector solicita todas las credenciales necesarias por el colaborador para el desempeño de su labor, entre esas la cuenta de google, de	En el periodo se cubrió todos los funcionarios y contratistas que han hecho reporte a mesa de servicio sobre novedades correo.	<p>1. En el periodo se realizó la adquisición de 250 cuentas de microsoft y se ejecutó migración.</p> <p>2. Se verificó la destinación y gestión de las cuentas disponibles, realizando la validación y asignación de las mismas y se implementan los Controles de</p>	<p>El control definido no cumple con la estructura de: Responsable de ejecutar el control + acción + complemento, de acuerdo con instrucciones de la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" Versión 6.</p> <p>Dentro de los seguimientos se</p>

		acuerdo con lo descrito en el procedimiento Administración de Usuarios para Servicios y Sistemas de información (E-05-002)		Acceso a la Información a través de mesa de servicio, para lo cual se generan tickets de casos. 3. Se estableció lineamiento para la asignación de usuarios dentro del procedimiento E-05-P-015 Creación y Deshabilitación de Usuario del Directorio Activo.	sugiere describir cuantos usuarios y cuantas licencias tiene la entidad, con el fin de contar con la referencia de los datos allí registrados, para determinar si se está cumpliendo con el licenciamiento <i>versus</i> usuarios.
--	--	--	--	--	--

Fuente: Matriz de riesgos Aprobación CIGD 10 2023-07-18, y observaciones de la auditora

🚩 Tipo(s) de riesgo(s) de Fraude - un (1) riesgo

Referencia	RIESGO	CONTROL	Periodo: Cuatrimestre Q1 2023	Periodo: Cuatrimestre Q2 2023	OBSERVACIONES OCI
			Descripción del Avance, Evidencia y/o Observaciones	Descripción del Avance, Evidencia y/o Observaciones	
132	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	El Profesional de Seguridad de la Información capacita a todo el personal del INM sobre la clasificación y valoración de los activos de Información con el fin de mitigar las fallas en la identificación y valoración de los mismos. La OIDT cuenta con el procedimiento Gestión de Activos de información (E-05-P-004) en el cual se establecen los lineamientos y actividades necesarias	Se realizó capacitación del procedimiento de Gestión de Activos de información (E-05-P-004) a todo el personal del INM los días 24 y 27 de abril, con el objetivo de dar inicio a la actualización de la matriz de activos. Se tienen listados de asistencia.	En el periodo se ejecutaron las siguientes actividades relacionadas con los controles: 1. Se realizó actualización del procedimiento E-05-P-004 Gestión de activos de la Información. 2. Se actualizó la matriz de activos y se dio aprobación en CIGD 10 del 18 de julio. 3. Se elaboró Instructivo E-05-I-024 de etiquetado de la información y se realizó socialización en el mes de agosto.	No se aportó evidencia que permita observar el cumplimiento de la capacitación a todo el personal de la INM, pero si se observa que se cuenta con la matriz de activos de información. Por lo anterior, se sugiere que se mejore el levantamiento de evidencias.

		para la gestión de activos de información dentro del marco de seguridad y privacidad de la información del INM			
--	--	--	--	--	--

Fuente: Matriz de riesgos Aprobación CIGD 10 2023-07-18, y observaciones de la auditora

🚩 Tipo(s) de riesgo(s) Gerencial - un (1) riesgo

Referencia	RIESGO	CONTROL	Periodo: Cuatrimestre Q1 2023	Periodo: Cuatrimestre Q2 2023	OBSERVACIONES OCI
			Descripción del Avance, Evidencia y/o Observaciones	Descripción del Avance, Evidencia y/o Observaciones	
120	Posibilidad de afectación económica y reputacional por inexistencia de soporte técnico para las herramientas tecnológicas del INM debido a la baja planificación y control sobre la infraestructura tecnológica de la entidad	El profesional asignado por el Jefe de la OIDT define y actualiza dentro de su proceso de TI, políticas de soporte para las herramientas tecnológicas del INM con el fin de mejorar la planificación en cuanto al soporte	1. La OIDT brindó soporte a las herramientas tecnológicas del INM durante el primer cuatrimestre de la vigencia 2023 de acuerdo con las necesidades de la entidad y siguiendo lo establecido en el procedimiento de Gestión de Incidentes y Requerimientos de Servicios de TI (E-05-P-003). Adicionalmente, se atendieron 118 casos de software instalado en laboratorios y oficinas, como el office o de licencia libre: R studio, Mendeley, labview, Schip, Google drive, zotero, forticlient, hbm catman, obs, mboxviewer, project, thunderbird, storm-elogic, stormusercgr, adobe reader, active campaign, vlc, solid works, filezilla, vaisala.	En el periodo se ejecutaron las siguientes actividades relacionadas con los controles: 1. En el periodo se realizó actualización del procedimiento E-05-P-003 Gestión de Incidentes y Requerimientos de Servicios de TI y Anexo de matriz de escalamiento, se ajustaron controles que permitan dar seguimiento a los servicios y tiempos de respuesta prestados por la OIDT estableciendo el uso de GLPI para la recepción de incidentes y requerimientos. 2. Adicionalmente se actualizaron las políticas establecidas en el procedimiento E-05-P-011 Procedimiento Control De Acceso A Los Servicios Tecnológicos Y Sistemas De Información Del	Respecto al control, se recomienda revisar la acción del profesional dado que por responsabilidades no es quien define políticas en una entidad, lo anterior de acuerdo a la ley 489 de 1998 " <i>Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.</i> ". Adicional, el control no indica que pasa con las desviaciones que se puedan presentar en el momento de la prestación del servicio; tal y como

			<p>2. En el periodo se solucionaron requerimientos en cuanto a aplicativos de BPMetro y SGDEA, se atendieron 105 casos de los cuales 79 se encuentran cerrados y los restantes en gestión del proveedor Digital Ware, sin embargo, en el periodo se evidenció que para Bpmetro se tienen pendiente la solución de 4 casos sobre el servicio de ensayo de aptitud y tres de PQRS, para los cuales se realiza seguimiento.</p>	<p>INM. 3. Se creo el procedimiento E-05-P-015 Creación y Deshabilitación de Usuario del Directorio Activo.</p>	<p>se evidenció en muestra de servicios prestados: a) Solicitud de instalación de wifi que en la matriz se indica que el tiempo de solución corresponde de 15 mm a 480 min; sin embargo en los casos de:9973, 9721, 9210, se excede en estos tiempos. b) Asignación de VPN se tiene un tiempo estipulado entre 30 min y 180 min; sin embargo los casos: 10685, 10562, 8989, 8352, se excede en estos tiempos. c) backups, que el tiempo estimado se encuentra entre 15 min y 1440 min; sin embargo en los servicios: 7992, 11566, 10838, se excede en estos tiempos.</p> <p>Por lo anterior, se recomienda que se mejore el análisis de este control para que realmente se vea la efectividad.</p>
--	--	--	--	---	--

Fuente: Matriz de riesgos Aprobación CIGD 10 2023-07-18, y observaciones de la auditora

🚩 Tipo(s) de riesgo(s) Operativo - cinco (5) riesgos

Referencia	RIESGO	CONTROL	Periodo: Cuatrimestre Q1 2023	Periodo: Cuatrimestre Q2 2023	OBSERVACIONES OCI
			Descripción del Avance, Evidencia y/o Observaciones	Descripción del Avance, Evidencia y/o Observaciones	
122	Posibilidad de afectación económica y reputacional por fallas en los aplicativos del INM debido a que no se	El profesional asignado por el Jefe de la OIDT, cada vez que se realiza un cambio o desarrollo nuevo, configura los ambientes de desarrollo y pruebas	1. En el periodo no se avanzó en nuevos desarrollos, se realizaron únicamente actividades de mantenimiento	En el periodo se ejecutaron las siguientes actividades relacionadas con los controles: 1. Se tiene un nuevo servidor de	Dentro de las evidencias aportadas se observa: *Control 1: Se presenta de

	<p>garantizan los requisitos mínimos (infraestructura, seguridad de la información, requerimientos de software) durante el desarrollo de estos.</p>	<p>en el servidor de aplicaciones principal y alterno, restringe el acceso a la Información y actualiza y mantiene el sistema de respaldo (Backups) de los aplicativos de la entidad con el fin de mitigar las fallas de los aplicativos en los ambientes de producción</p> <p>La OI DT cuenta con el instructivo metodología para el Ciclo de Vida de Desarrollo de Software de INM (E-05-I-021) donde se establecen los requisitos para evaluar y aprobar de manera correcta los requisitos mínimos para el desarrollo de software</p>	<p>de software. 2. En el periodo se aseguró el cumplimiento de los controles referentes a backups e infraestructura tecnológica.</p>	<p>aplicaciones en producción y un entorno con características de desarrollo, posteriormente se pasa al entorno de producción. Se da cumplimiento al control 2. Se realizó respaldo a la base de datos de los servicios y se realizan backups diarios de la información. 3. En el periodo se actualizaron las políticas de copias de respaldo de la información con la generación de la versión 1 del procedimiento E-05-P-014 Generación, Administración y Restauración de Copias de Respaldo de la información.</p>	<p>backups realizados; lo que no permite ver la totalidad del control.</p> <p>*Control 2; se sugiere mejorar la redacción, dado que los equipos no se mantienen en constante movimiento; adicional las planillas que fueron suministradas como evidencia, no se encuentran completamente diligencias.</p> <p>*Control 3: Se aportó el documento con código E-05-F-027 Instructivo de Usuario de SISEPM 2.0 para lo cual se evidencia que tomaron el formato equivocado.</p> <p>En caso de que este documento sea borrador, se recomienda implementar la marca de agua borrador. Adicional no se logra identificar como se garantiza el servicio, es por ello que se debe mejorar el levantamiento de evidencias.</p>
		<p>El profesional asignado por el Jefe de la OI DT ubica y protege los equipos tecnológicos, elementos de protección y control ambiental e implementa un perímetro de seguridad física de los mismos y realiza seguimiento mensual</p>	<p>En el periodo no se materializó el riesgo, el seguimiento que se realiza esa las condiciones ambientales y autorización de ingreso y salida del datacenter.</p>	<p>En el periodo no se materializó el riesgo, el seguimiento que se realiza en las condiciones ambientales y autorización de ingreso y salida del datacenter. Se realizó mantenimiento al aire acondicionado del data center lo cual permitió asegurar las condiciones ambientales.</p>	
		<p>El profesional especializado asignado por el Jefe de la OI DT garantiza el soporte y atención de las posibles fallas que se puedan presentar en los aplicativos desarrollados en el INM y los desarrollados por</p>	<p>1. Se atendieron 972 casos relacionados con requerimientos de desarrollos internos a los cuales se les dio tratamiento. 2. Referente a terceros</p>	<p>1. Se ha dado cumplimiento a diferentes requerimientos de SASM y otros mantenimientos de aplicativos internos. Se atendieron 271 casos relacionados con requerimientos de desarrollos y/o mantenimientos</p>	

		<p>terceros y garantiza que se cuente con manuales de los aplicativos y/o documentos equivalentes que ayuden a dar soporte debido a algún incidente o falla</p>	<p>(proveedores) se atendieron 105 casos de los cuales 79 se encuentran cerrados y los 26 restantes en gestión por parte de los proveedores de BPMetro y SGDEA, sin embargo, en el periodo se evidenció que para Bpmetro se tienen la solución de cuatro: 4 casos sobre el servicio de ensayo de aptitud y tres de PQRS.</p>	<p>internos a los cuales se les dio tratamiento. El indicador se cumplió en un 93% encontrándose en nivel satisfactorio. 2. Se brindó soporte a software desarrollado por externos BPMetro, SGDEA y KACTUS a través de la ejecución de los contratos No. 074 y 040, con indicadores de cierre de casos del 91% y 100% respectivamente, dando cumplimiento a las obligaciones establecidas, de conformidad a los informes de supervisión.</p>	
<p>125</p>	<p>Posibilidad de afectación reputacional por intermitencias en la prestación de servicios de TI prestados por terceros debido al incumplimiento de las obligaciones contractuales</p>	<p>Los supervisores de contrato realizan seguimiento de los acuerdos de servicio establecidos (ANS) con las herramientas de monitoreo correspondientes, a los servicios críticos "internet, correo" prestados por terceros (obligaciones contractuales), con el fin de monitorear la calidad de los servicios.</p> <p>Para la contratación y seguimiento de los contratistas, todos los procesos de la entidad aplican lo establecido en el proceso de Contratación.</p>	<p>En el periodo se dio cumplimiento de los ANS por parte del proveedor de internet y correo, se tienen informes de supervisión de cumplimiento a obligaciones contractuales.</p>	<p>1. En el periodo se dio cumplimiento de los ANS por parte del proveedor de internet, se tienen informes de supervisión de cumplimiento a obligaciones contractuales.</p> <p>2. Se realizó migración a microsoft. No se han presentado quejas en cuenta a la migración y nuevo proveedor de correo electrónico. Se tienen informes de supervisión.</p>	<p>El Control requiere que sea más específico, dado que se indica "[...]Los supervisores de contrato [...]; este es muy ambiguo dado que no permite determinar cuántos son los supervisores, o acotar en cuantas personas esta la supervisión. Lo que no permite medir la efectividad.</p> <p>En cuanto al registro del seguimiento, tampoco se describe de que contratos están ejecutando el control (1er seguimiento), para el segundo si se describe escuetamente las actividades.</p> <p>Ahora bien, dentro</p>

					de las evidencias se adjuntaron para el contrato de Microsoft: Actas de inicio, y listado de licencias instaladas (247 registros), el pantallazo de activación de licencias. Mientras para el servicio de internet, se aportaron los informes de supervisión de los meses, 3,4,5,6,7,9 y 11; estos permiten evidenciar que se están ejecutando el control sin embargo se observa que falta evidencia de algunos meses.
126	Posibilidad de afectación económica por exposición (daño o pérdida) de dispositivos informáticos a condiciones e instalaciones inadecuadas debido a la baja gestión en el seguimiento y control de los mismos.	El profesional asignado por el Jefe de la OI DT ubica y protege los equipos tecnológicos, elementos de protección y control ambiental e implementa un perímetro de seguridad física de los mismos y realiza seguimiento mensual	1. Durante el primer cuatrimestre de la vigencia 2023 no se evidenciaron incidentes de TI relacionados con daño o pérdida de dispositivos informáticos. 2. El seguimiento que se realiza es el seguimiento a las condiciones ambientales y autorización de ingreso y salida del datacenter.	1. Durante el segundo cuatrimestre de la vigencia 2023 no se evidenciaron incidentes de TI relacionados con daño o pérdida de dispositivos informáticos. 2. En el periodo no se materializó el riesgo, el seguimiento que se realiza en las condiciones ambientales y autorización de ingreso y salida del datacenter. Se realizó mantenimiento al aire acondicionado del data center lo cual permitió asegurar las condiciones ambientales.	Se recomienda ajustar la redacción del control, pues se indica "[...]El profesional asignado por el Jefe de la OI DT ubica y protege los equipos tecnológicos [...]"(subrayado fuera del texto). La entidad debe contar con un mapeo de los equipos y puntos de red, así como los puestos de trabajo; lo que hace que estos puntos son fijos y no se pueden movilizar; al no ser que se encuentren remodelación y se reubiquen. Ahora bien, el término de <u>proteger</u> tiene mucho contexto y no es específico, ¿lo protege de robos?, lo protege del mal uso?, ¿lo protege de alteraciones?,

					<p>entre otras situaciones. Es por lo que el control debe sea claro y concreto para poderse validar. En este sentido es muy difícil indicar que este control este dando el resultado esperado.</p> <p>Adicional, en el registro de seguimiento y la evidencia, no describe como se implementa un perímetro de seguridad física en la entidad; y su registro al ser cuatrimestral no se detalla de manera mensual tal y como se describe en el control.</p>
127	<p>Posibilidad de afectación económica por la incorporación de tecnología en los diferentes procesos del INM que no cumplen con los requerimientos para garantizar la conectividad con la plataforma tecnológica existente debido a que no existe una adecuada interrelación entre los diferentes procesos de la entidad con la OIDT</p>	<p>El profesional asignado por el Jefe de la OIDT, atiende las solicitudes de nuevos proyectos con el fin de evitar la adquisición de sistemas no compatibles</p> <p>La OIDT cuenta con el procedimiento Atención de Requerimientos de Mantenimiento de Software (E-05-P-001) donde establece los criterios para la presentación, estudio y atención de requerimientos de mantenimiento, ajuste o mejoramiento de aplicativos de software desarrollados por el INM y el instructivo metodología para el Ciclo de Vida de Desarrollo de Software de INM (E-</p>	<p>1. Se iniciaron mesas para la actualización de la documentación de desarrollo de software.</p> <p>2. Se adelantó la etapa precontractual (estudios previos y de mercado) para la adquisición de software de inventarios a través del proyecto de inversión, el cual se espera su ejecución para el siguiente cuatrimestre.</p> <p>3. Se atendieron 972 casos de mantenimiento a los desarrollos internos a los cuales se les dio tratamiento.</p>	<p>En el periodo se ejecutaron las siguientes actividades relacionadas con los controles:</p> <p>1. Se está trabajando en actualización de materiales de referencia, módulo para medición de materiales de referencia, módulo de recaudos.</p> <p>2. Se realizó adquisición de software de inventarios, el cual se encuentra en implementación hasta el mes de diciembre. En el mes de octubre se prevee el término de cargue de información e inicio de producción. En la adquisición de este software se da cumplimiento a lo establecido en el</p>	<p>Este control permite evidenciar las actividades realizadas en la implementación de nuevas soluciones, como es el caso de NOVASOFT, donde la evidencia permite al auditor conocer las etapas que se contemplaron y el seguimiento realizado para su implementación; para el caso de SISEPM, no se aporta evidencia, ni reporte de los casos de mantenimiento de desarrollos realizados.</p> <p>Por lo anterior, se recomienda mejorar la construcción de las evidencias para demostrar el cumplimiento del control definido.</p>

		<p>05-I-021) donde se establecen los requisitos para evaluar y aprobar de manera correcta los requisitos mínimos para el desarrollo de software</p>	<p>4. Durante el primer cuatrimestre de la vigencia 2023 no se incorporaron nuevas tecnologías en los diferentes procesos de la entidad.</p>	<p>procedimiento E-05-P-013 Procedimiento Adquisición, Desarrollo y Mantenimiento de Software y Automatización de Mediciones 3. Durante el segundo cuatrimestre de la vigencia 2023 no se incorporaron nuevas tecnologías en los diferentes procesos de la entidad.</p>	
<p>130</p>	<p>Posibilidad de afectación reputacional por no dar respuesta oportuna a los incidentes y requerimientos de servicios de TI, reportados por los usuarios internos a la Mesa de Servicio del INM debido a una mala gestión de los Incidentes y Requerimientos de TI por parte del líder de la Mesa de Servicio</p>	<p>Los profesionales de la Mesa de Servicio resuelven los incidentes y/o requerimientos de servicio de TI, de acuerdo con los ANS establecidos por la entidad en el Anexo 2 Matriz de Prioridad, Escalamiento y Tiempos de Respuesta del procedimiento E-05-P-003 Gestión de Incidentes y Requerimientos de Servicios de TI</p> <p>Los incidentes o requerimientos son tratados y resueltos por medio de la Mesa de Servicio mediante la herramienta GLPI la cual se encuentra debidamente parametrizada</p>	<p>1. Se registraron durante el cuatrimestre 2247 solicitudes en la herramienta GLPI, de los cuales 1859 se atendieron dentro de los ANS y 388 por fuera de los tiempos debido a la falta de personal en el área de soporte para niveles I, II y III durante el mes de enero y a la coyuntura del ingreso y salida de personal por el concurso de méritos, por lo tanto se obtuvo un cumplimiento del indicador del 83%, el cual se encuentra en un nivel satisfactorio. Se aclara que los casos pendientes fueron atendidos durante el periodo y no se presentaron quejas por el</p>	<p>Se registraron durante el cuatrimestre 3061 solicitudes en la herramienta GLPI, de los cuales 2561 se atendieron dentro de los ANS y 388 por fuera de los tiempos, por lo tanto se obtuvo un cumplimiento del indicador del 83%, el cual se encuentra en un nivel satisfactorio. Se aclara que los casos pendientes fueron atendidos durante el periodo y no se presentaron quejas por el incumplimiento presentado, ni fueron de impacto negativo para los servicios. Se tiene informes mensuales de mesa de servicio de mayo a agosto.</p>	<p>Este control permite evidenciar que se está realizando el seguimiento a los reportes de Incidentes y/o requerimientos efectuados a la mesa de ayuda; sin embargo, como evidencia solo se aportó el informe correspondiente al mes de mayo. Este informe relaciona las diferentes actividades realizadas por la mesa de ayuda; pero las conclusiones indican más un resumen más que una conclusiones. Adicional no se describe que plan adelantan con los casos que se traen acumulados y que no cumplen con los tiempos de atención.</p> <p>Para el segundo cuatrimestre se registra en el seguimiento que fueron 388 casos que se atendieron fuera de los tiempos establecidos.</p>

			incumplimiento presentado, ni fueron de impacto negativo para los servicios.		Se recomienda, que se indique que acciones adicionales se toman para bajar estas cifras, en las diferentes categorías y si estas se pueden llevar a gestión del conocimiento para continuar mejorando tiempos de respuesta.
--	--	--	--	--	---

Fuente: Matriz de riesgos Aprobación CIGD 10 2023-07-18, y observaciones de la auditora

Tipo(s) de riesgo(s) de Seguridad Digital - dos (2) riesgos

Referencia	RIESGO	CONTROL	Periodo: Cuatrimestre Q1 2023	Periodo: Cuatrimestre Q2 2023	OBSERVACIONES OCI
			Descripción del Avance, Evidencia y/o Observaciones	Descripción del Avance, Evidencia y/o Observaciones	
121	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).	<p>El profesional asignado por el Jefe de la OIDT, define las herramientas informáticas para la protección ante posibles amenazas existentes con el fin de asegurar la continuidad de la seguridad de la información</p> <p>El profesional de Seguridad de la Información ha definido e implementando políticas para la seguridad de la información al interior de la entidad (Manual Técnico del SGSI E-05-M-002)</p>	<p>En el periodo se realizaron acciones de mantenimiento de los equipos de seguridad perimetral como el firewall y fortinet lo que han evitado que se realicen ataques informáticos a la entidad.</p> <p>En el periodo se realizó actualización del plan de tratamiento de riesgos de seguridad de la información e inició la actualización de políticas descritas en el Manual de Seguridad y Privacidad de la Información. Se</p>	<p>En el periodo se realizó actualización de las políticas de seguridad de la información contenidas en el Manual Técnico del Sistema de Seguridad de la Información y el procedimiento de E-05-D-004 Infraestructura y Redes.</p> <p>En el periodo se realizó actualización de las políticas de seguridad de la información contenidas en el Manual Técnico del Sistema de Seguridad de la Información y el procedimiento de E-05-D-004 Infraestructura y Redes. Se realiza</p>	<p>Frente a este riesgo, que cuenta con dos (2) controles Control 1: Se recomienda cambiar el término "definir", dado que el profesional no define herramientas. Ahora bien, en cuanto al seguimiento del segundo cuatrimestre, se describe que se actualizó el <i>Manual Técnico del Sistema de Seguridad de la Información y un procedimiento</i>; pero esas actividades no apuntan al control. Pues no se describe frente a los ataques informáticos que pudieron haber afectado la disponibilidad de la información.</p> <p>Control 2: Se recomienda cambiar el término "definir", dado que el profesional no define</p>

			cuenta con seguimiento presentado en CIGD del 24 de abril.	control a través de mesa de servicio y el profesional especializado 14 de conformidad con las funciones.	<p>políticas. En cuanto al seguimiento, se reporta la actualización de los documentos que son importantes para la operación, pero estos no me permiten evidenciar que políticas fueron revisadas y si fueron efectivas.</p> <p>La evidencia aportada del registro de ticket en mesa de servicio, y el registro de actualización de documentos en Isolución del todo no permiten evidenciar que esos controles sean los correctos para que no se materialice el riesgo.</p>
124	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	<p>El Profesional designado por el Jefe de la OI DT mantiene el soporte del firewall y de la plataforma de antivirus y establece restricciones de acceso a la información con el propósito de proteger la infraestructura crítica del INM</p> <p>La OI DT cuenta con el procedimiento Administración de Usuarios para Servicios y Sistemas de información (E-05-002) donde se establecen los Controles de Acceso a la Información</p>	<p>1. El firewall se encuentra actualizado en el periodo, su fecha de vencimiento es en el mes de junio, y se están adelantando las gestiones pertinentes para su renovación. En cuanto al antivirus, este se encuentra también vigente y su fecha de vencimiento está para el 2 de febrero de 2024. Lo anterior ha permitido la protección de la infraestructura crítica del INM.</p> <p>2. Se implementan los Controles de Acceso a la Información con el formato E-05-F-003 Reporte de Novedades de Usuario para</p>	<p>En el periodo se ejecutaron las siguientes actividades relacionadas con los controles:</p> <p>1. En el periodo se ejecuto contrato 114 de 2023 sobre el servicio de renovación del soporte y extensión de garantía de equipos FORTINET para mantener la infraestructura tecnológica del INM, lo cual permitio tener protección al acceso de la información.</p> <p>2. Se ejecuta control de la consola, a la fecha no se ha presentado amenazas.</p> <p>3. En cuanto al antivirus, este se encuentra también vigente y</p>	<p>Este riesgo, cuenta con un (1) control y se recomienda, cambiar el término "mantener", dado que el profesional no mantiene el soporte del firewall, ahora bien, en cuanto al registro de seguimientos, se describe que se ha realizado la protección de la información e indica que el antivirus se encuentra actualizado y se efectúa el monitoreo en la consola de Fortinet. Como evidencia se aportó pantallazo de consola, listado de ticket y listado de documentación actualizada.</p>

			Sistemas de Información y Servicios Tecnológicos a través de mesa de servicio. En el periodo no se identificó acceso a la información de usuarios no autorizados.	su fecha de vencimiento esta para el 2 de febrero de 2024, se ha adelantado estudios previos para su renovación. Lo anterior ha permitido la protección de la infraestructura crítica del INM.	
--	--	--	---	--	--

Fuente: Matriz de riesgos Aprobación CIGD 10 2023-07-18, y observaciones de la auditora

🚩 Tipo(s) de riesgo(s) Tecnológico - cuatro (4) riesgos.

Referencia	RIESGO	CONTROL	Periodo: Cuatrimestre Q1 2023	Periodo: Cuatrimestre Q2 2023	OBSERVACIONES OCI
			Descripción del Avance, Evidencia y/o Observaciones	Descripción del Avance, Evidencia y/o Observaciones	
118	Posibilidad de afectación económica y reputacional por el uso de software obsoleto o desactualizado para la operación de los procesos del INM debido a fallas en la administración del software implementado.	El profesional asignado por el Jefe de la OIDT hace seguimiento a través del inventario de software implementado en el INM con el fin de evitar el uso no intencionado de software desactualizado e identificar necesidades de actualización del mismo. La OIDT cuenta con el procedimiento Atención	1. Se tiene un inventario de software en GLPI en el cual se realiza seguimiento. Adicionalmente, se realizó control de los software instalados en las áreas a través de solicitud de permisos de administrador. 2. Todos los requerimientos relacionados con el mantenimiento, ajuste o mejora de los Sistemas de Información (Software) se realizan de acuerdo con lo establecido en el procedimiento de Atención de Requerimientos de Mantenimiento de Software. Durante el primer cuatrimestre de la vigencia 2023 no se evidencian requerimiento de TI asociados a software desactualizado. Durante este periodo se identificó que actualmente el servidor instalado en el 2018 de servicios en línea, y las aplicaciones desarrolladas internamente, presenta obsolescencia y además tiene fallas a nivel de hardware que puede repercutir en un riesgo, por lo cual se iniciaron gestiones en abril para acondicionar un nuevo servidor virtual de última tecnología. 3. El indicador "Requerimientos de Desarrollo y Mantenimiento de	En el periodo se ejecutaron las siguientes actividades relacionadas con los controles: 1. Se actualizó el procedimiento por lo tanto, se eliminó y se generó la versión 1 del E-05-P-013 Procedimiento Adquisición, Desarrollo y Mantenimiento de Software y Automatización de Mediciones, donde se establecen nuevos	El Control definido, se observa que se está aplicando de manera adecuada, ya que se cuenta con el inventario de sistemas de información con 64 registros y software de gestión con 30 registros. Adicional en los seguimientos se registra las diferentes actividades para garantizar que el control se está aplicando de manera adecuada.

		<p>de Requerimientos de Mantenimiento de Software (E-05-P-001) donde establece los criterios para la presentación, estudio y atención de requerimientos de mantenimiento, ajuste o mejoramiento de aplicativos de software desarrollados por el INM</p>	<p>Software" se ha cumplido a satisfacción con un resultado promedio del 94%.</p>	<p>controles de seguridad y se actualizó el catálogo de sistemas de información de la entidad E-05-F-033. 2. A la fecha se ha dado cumplimiento a los indicadores en un 93% y 100%. 3. Se inicio actualización del SISEPM, SASM y otros módulos, a través del contrato No. 028 de 2023 por medio del cual se contrató profesional desarrollador. 4. La actualización y mantenimiento de los sistemas de información BPMetro y SGDEA se asegura a través del contrato Contrato 074 de 2023 2 Contratar el Soporte, Mantenimiento y Actualización de las Plataformas Ophelia-SGDEA y Ophelia-Bpmetro del Instituto Nacional de Metrología" (con proveedor externo)</p>	
--	--	---	---	--	--

				incluyendo actualizaciones de lenguajes de programación, servidores, funciones entre otras actividades que sirven de mejora.	
119	Posibilidad de afectación económica y reputacional por el uso de hardware obsoleto o desactualizado para la operación de los procesos del INM debido a una baja gestión en el seguimiento y control del estado del hardware utilizado	<p>El profesional asignado por el Jefe de la OI DT revisa el inventario del hardware del INM donde se evidencian los ciclos de vida de los equipos y elementos tecnológicos con el fin de visualizar el soporte y periodo de vida de los equipos informáticos</p> <p>El profesional asignado por el Jefe de la OI DT genera reporte del estado del Hardware utilizado en el INM con el fin de visualizar el soporte y periodo de vida en equipos informáticos</p>	<p>1. El inventario del Hardware se controla mediante la herramienta GLPI a través del cual se realiza el seguimiento correspondiente al ciclo de vida de los equipos y elementos tecnológicos. Ver http://192.168.10.103/glpi/index.php?noAUTO=1</p> <p>2. En el periodo se adelantó informe de obsolescencia de equipos con el fin identificar necesidades para adquirir nuevos equipos a través del proyecto de inversión.</p>	<p>1. Se realizó actualización del inventario, y se emitió concepto por obsolescencia. Este inventario se encuentra actualizado en GLPI: para equipos, periféricos y consumibles, lo que permite realizar monitoreo y seguimiento.</p> <p>2. Se realizó actualización del inventario obsoleto y se informó al jefe OI DT, con el fin de dar gestión por medio de almacén para baja. Adicionalmente se tiene programado realizar compra de equipos de cómputo de mesa y portátiles, por otra parte, se realizó una primera</p>	<p>Este riesgo cuenta con tres (3) controles: * Control 1: Para este control no se aportó evidencia, en ninguno de los dos periodos de seguimiento, al igual no se registró cuál es el porcentaje de obsolescencia en materia de equipos dentro de la entidad.</p> <p>* Control 2: No se aporta evidencia que permita observar la aplicación del control, y en los seguimientos no se indica que % de obsolescencia tiene la entidad en materia de hardware.</p> <p>*Control 3: Si bien describen el seguimiento de las actividades realizadas, no se aportó la evidencia para su revisión. En cuanto al mantenimiento preventivo se</p>

				<p>adquisición por bolsa de repuestos para la compra de periféricos y repuestos Contrato 116 de 2023, lo anterior a asegurado que se realice cambio de tengan herramientas para el cambio de hardware que presente fallas.</p>	<p>indica que se encuentra en proceso de levantamiento de estudios previos.</p>
		<p>El contratista designado realiza mantenimiento preventivo a la infraestructura tecnológica del INM anualmente con el fin de detectar la necesidad de mantenimiento, ajuste o mejora del hardware utilizado en los diferentes procesos de la entidad</p> <p>La OI DT cuenta con el procedimiento de gestión de Incidentes y Requerimientos de Servicios de TI (E-05-P-003) que especifica el</p>	<p>1. El mantenimiento preventivo de la infraestructura tecnológica se realiza de manera anual, ésta se encuentra programada para el mes de septiembre.</p> <p>2. En el periodo a través del procedimiento gestión de Incidentes y Requerimientos de Servicios de TI (E-05-P-003), se solucionaron los siguientes incidentes por fallas de hardware: 15 mantenimientos, 13 cambio de teclados, entregando uno de cambio, 8 por fallas en puertos de entrada y salida, 4 por fallas en mouse, 1 revisión de board, 7 por falla en monitores, 2 por lentitud de equipo, se realizó 17 formateos de equipos que presentaron fallas, 1 mantenimiento de impresora, para un total de 103 requerimientos y se realizaron 7 conceptos técnicos de equipos para baja, que por su obsolescencia ya no funcionaban.</p>	<p>En el periodo se ejecutaron las siguientes actividades relacionadas con los controles:</p> <p>1. Por parte de mesa de servicio se ha realizado mantenimientos preventivos dirigidos por solicitud a través de GLPI a equipos y periféricos que presentan fallas. Se ha dado respuesta oportuna a los requerimientos.</p> <p>2. Se ha adelantado gestión para la contratación de compra de equipos para renovación</p>	

		proceso para comunicar de manera oportuna a la Mesa de Servicio del INM la necesidad de mantenimiento, ajuste o mejora del hardware utilizado en los diferentes procesos de la entidad		de los que se ha identificado su obsolescencia y se tiene programada su adjudicación para el mes de Septiembre, con esto se asegurará que las áreas cuenten con equipos actualizados y de mayor capacidad. 3. Se adelanta la elaboración de estudios previos para la contratación de mantenimiento de la infraestructura tecnológica por un valor de 38.000.000, se está a la espera de actualización de CDP y aprobación de ficha del proyecto de inversión.	
128	Posibilidad de afectación económica y reputacional por imposibilidad de recuperación de información en los diferentes procesos de la entidad debido al poco control	El profesional de Seguridad de la información refuerza el conocimiento y aplicación de políticas y buenas prácticas de respaldo de la información con el fin de	<ol style="list-style-type: none"> 1. En el periodo no se presentó pérdida de información, se implementaron los controles del procedimiento Backups y Restauración de Información en Equipos de Cómputo y Servidores (E-05-P-002) y se realizaron trece copias de respaldo de la información contenidas en diferentes servidores de la entidad. 2. Se actualiza el plan operativo de seguridad y privacidad de la información mediante CIGD N° 5 del 2023-03-29 y 2023-04-04, en el cual se establecen actividades de sensibilización. 	En el periodo se ejecutaron las siguientes actividades relacionadas con los controles: 1. Establecimiento de nuevas políticas a través de la elaboración del procedimiento	Este riesgo cuenta con dos (2) controles: *Control 1: De acuerdo con descripción del control parece que solo se aplicará para el profesional que ejecuta el control, y no para toda la entidad. Se recomienda mejorar su

	<p>sobre las directrices descritas en los procedimientos, instructivos y/o guías establecidas en el proceso de TI</p>	<p>minimizar el riesgo de pérdida de información</p> <p>El profesional asignado por el Jefe de la OIDT realiza copias de respaldo de la información de acuerdo con lo establecido en el procedimiento Backups y Restauración de Información en Equipos de Cómputo y Servidores (E-05-P-002)</p>		<p>o E-05-P-014 Generación, Administración y Restauración de Copias de Respaldo de la información el cual reemplazó el E-05-P-002 procedimiento Backups y Restauración de Información en Equipos de Cómputo y Servidores.</p> <p>2. En el periodo no se presentó pérdida de información, se implementaron los controles del procedimiento E-05-P-014 Generación, Administración y Restauración de Copias de Respaldo de la información y se realizaron 12 copias de respaldo de la información contenidas en diferentes servidores de la entidad.</p> <p>3. Se adquirió una solución de backup para respaldo de información y servidores para actualizar la</p>	<p>redacción y finalidad.</p> <p>*Control 2: Para el primer seguimiento, se observa en archivo "1.6.128.2 backups.xlsx", en pestaña 2023, se registran tan solo nueve (9) registros de backups. Lo que no permite evidenciar el cumplimiento de la elaboración de los backups. Además, en archivo "1.6.128.2 restauración.csv" se observa 17 registros de solicitudes de restauración de backups.</p> <p>De otra parte, se registró como seguimiento que se adquirió una solución de backup.</p>
--	---	---	--	---	--

				infraestructura tecnológica del INM a través del contrato 148 de 2023. En el periodo se adelantó gestión con el proveedor para revisión y diagnóstico e inicio de ejecución.	
131	Posibilidad de afectación económica y reputacional por afectación en la Seguridad de la Información al realizarse trabajo en casa debido a la falta o incumplimiento de políticas y buenas prácticas de Seguridad de la información relacionadas con el Trabajo en Casa.	<p>El Profesional de Seguridad de la Información concientiza a los usuarios sobre los riesgos de pérdida o daño de los computadores utilizados por los funcionarios para desarrollar actividades de trabajo en casa</p> <p>El Profesional de Seguridad de la Información periódicamente concientiza a los usuarios sobre buenas prácticas de Seguridad de la Información relacionadas con el Trabajo en Casa</p>	<p>En el periodo no se asignaron equipos de cómputo a funcionarios y contratista para trabajo en casa.</p> <p>1. Se actualiza el plan operativo de seguridad y privacidad de la información mediante CIGD N° 5 del 2023-03-29 y 2023-04-04, en el cual se establecen actividades de sensibilización.</p> <p>2. Actualmente solo los contratistas realizan trabajo en casa, y se implementan los Controles de Acceso a la Información con el formato E-05-F-003 Reporte de Novedades de Usuario para Sistemas de Información y Servicios Tecnológicos a través de mesa de servicio. En el periodo no se identificó acceso a la información de usuarios no autorizados.</p>	<p>1. En el periodo no se asignaron equipos de cómputo a funcionarios y contratista para trabajo en casa.</p> <p>2. Se identifica que los subdirectores y jefes realizan solicitudes para llevar el equipo asignado por fuera de la entidad</p> <p>1. Se realizó capacitación en el mes de julio sobre la actualización de las políticas de seguridad de la información.</p> <p>2. Actualmente solo los contratistas realizan trabajo en casa, y se implementan los Controles de Acceso a la Información a través de mesa de</p>	<p>Este riesgo tiene definidos (2) controles: *Control 1: Se observa en reporte de ingreso y salida de equipos; pero no hay registro de actividades de concientización.</p> <p>Control 2: No se evidencia actividades periódicas sobre la seguridad de la información en el trabajo en casa.</p> <p>Se recomienda mejorar la descripción de los seguimientos de manera que si han salido equipos para el trabajo en casa, pero en su registro de seguimiento no está especificado, tal y como se observa en reporte abril 5,14.</p>

servicio, para lo cual se generan tickets de casos. En el periodo no se identificó acceso a la información de usuarios no autorizados.

Fuente: Matriz de riesgos Aprobación CIGD 10 2023-07-18, y observaciones de la auditora

Indicadores de la Dependencia

Consultada la información de indicadores en ISOLUCIÓN se observó:

Gestión de Tecnologías de la Información								95.555555556%
Indicador	Valor Real Acumulado	Tendencia	Meta	Valor real	Valor Estimado	Fecha medición	% Cumplimiento	Gráfica
% de Documentación del SGSI actualizada	90	↑	90	90	90	13/oct./2023	100 %	
% de implementación de controles de Seguridad de la Información	100	↑	80	100	100	13/oct./2023	100 %	
% de Sensibilizaciones ejecutadas en Seguridad de la Información	100	↑	90	100	100	13/oct./2023	100 %	
Actividades relacionadas en el PETI finalizadas dentro de las fechas programadas dando cumplimiento a los lineamientos y estándares establecidos en las Políticas de Gobierno y Seguridad Digital, de acuerdo con las directrices emitidas por MinTIC	58	↑	90	58	58	05/oct./2023	64.444444444 %	
Canal de datos institucional con una disponibilidad del 99.98% mensual garantizando la disponibilidad y continuidad de los servicios de la entidad y fortaleciendo de manera operativa los procesos organizacionales	99.98	↑	95	99.98	99.98	06/oct./2023	100 %	
Incidentes y Requerimientos de TI resueltos dentro de los tiempos establecidos en los Acuerdos de Nivel de Servicio (ANS) buscando la mejora continua en la gestión de TI y una mayor productividad de la entidad	86.68	↑	85	86.68	86.68	13/oct./2023	100 %	
Procesos de medición automatizados de acuerdo con las necesidades de la entidad que permitan la eficiencia y calidad de los procesos del INM	100	↑	90	100	100	13/oct./2023	100 %	
Requerimientos de Desarrollo y Mantenimiento de Software resueltos de acuerdo con las necesidades de arquitectura empresarial del INM garantizando la eficiencia y calidad de los procesos del INM	103.23	↑	80	103.23	103.23	13/oct./2023	100 %	

Fuente: Herramienta Isolución – módulo Indicadores

A continuación, se detalla por indicador así:

% de Documentación del SGSI actualizada:

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
13/oct./2023	90	90	90	85	75	A la fecha se han actualizado 17 documentos que hacen parte de los controles de Seguridad de la información de 23 planeados para el año, en el tercer trimestre se publicaron 9 de 10 programados: Documentos publicados 1. E-05-I-024 Etiquetado de Información 2. E-05-P-011 CONTROL DE ACCESO A LOS SERVICIOS TECNOLÓGICOS SISTEMAS DE INFORMACIÓN DEL INM 3. E-05-I-023 Apagado y Encendido de la Infraestructura de TI 4. E-05-P-014 Generación, Administración y Restauración de Copias de Respaldo de la información 5. Propuesta actualización de documento TH.docx 6. E-

05-P-015 Creación y Deshabilitación de Usuarios en el Directorio Activo 7. E-05-P-017 Gestión de Vulnerabilidades de Tecnologías de la Información 8. E-05-P-016 Mantenimiento de la Infraestructura Tecnológica 9. Instructivo Ath MFA en office 365.docx

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=NDAy&FechaIni=MjgvMTEvMjAyMg==&FechaFin=MjgvMTEvMjAyMg==>

De acuerdo con el contraste de información realizada en ISOLUCIÓN en el módulo de documentación, el documento: E-05-P-015 "Creación y Deshabilitación de Usuarios en el Directorio Activo", no se registra; adicional solo se describen nueve (9) documentos de los 17 que indican que se actualizaron, y el documento "5. Propuesta actualización de documento TH.docx", no se adjuntó, lo cual no permite validar la totalidad de los documentos actualizados.

% de implementación de controles de Seguridad de la Información

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
13/oct./2023	80	100	100	70	60	En el año se tiene programadas 12, a la fecha en total se han ejecutado 9. En el trimestre se ejecutaron 5 de las 5 capacitaciones programadas,. Las capacitaciones ejecutadas fueron: Políticas de seguridad de la información del INM, Políticas de seguridad de la información del INM para OIDT, Envío campaña de seguridad de la información por correo electrónico, Control de accesos.

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=NDA0&FechaIni=MjgvMTEvMjAyMg==&FechaFin=MjgvMTEvMjAyMg==>

Se aporta como evidencia:

Mis archivos > Auditoria de OTIC > INDICADORES > 1.8.8. % Implementación controles

Nombre	Modificado	Modificado por	Tamaño de arch...	Compartir
~\$guimiento a riesgos cuatrimestral.docx	20 de noviembre	Alba Graciela Rodríguez	162 bytes	Compartido
Boletin de seguridad.pdf	20 de noviembre	Alba Graciela Rodríguez	814 KB	Compartido
Seguimiento a riesgos cuatri...	20 de noviembre	Alba Graciela Rodríguez	65,2 KB	Compartido
Sesión capacitación politicas de seguridad...	20 de noviembre	Alba Graciela Rodríguez	334 KB	Compartido

Fuente: imagen de drive compartido para información compartida en la auditoría.

El objetivo de este indicador es: *“Definir, implementar, evaluar y mantener la gestión de Tecnologías de la Información a través del cumplimiento de los procedimientos establecidos en los componentes de la Estrategia de Gobierno Digital, de acuerdo a los lineamientos generados por MinTIC mediante la ejecución de planes y proyectos de inversión institucional, con el fin de fortalecer de manera estratégica y operativa la gestión del procesos del INM”*; lo que se puede observar, es que el seguimiento registrado no se encuentra alineado al objetivo del indicador, ni la evidencia da cuenta en su totalidad de la ejecución registrada.

% de Sensibilizaciones ejecutadas en Seguridad de la Información

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
13/oct./2023	90	100	100	80	70	En el año se tiene programados 8 controles para la mitigación de riesgos, los cuales se ejecutan de manera continua. En el trimestre se ejecutaron 5 de los 5 programados. Los controles ejecutados fueron: Establecer políticas de backups acorde a la criticidad de la información, Seguimiento a la aprobación de la TRD del proceso de control disciplinario, Establecer procedimientos de gestión de la operación de TI, Establecer políticas de seguridad para gestión de la operación de TI, Actualización de la matriz de riesgos, basado en los lineamientos de la guía del DAFP y la ISO27001:2022.

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=NDAz&FechaIni=MjkgMTEvMjAyMw==&FechaFin=MjkgMTEvMjAyMw==>

La evidencia aportada para este indicador es:

Mis archivos > Auditoria de OTIC > INDICADORES > 1.8.7. % Sensibilizaciones seg de la inf

Nombre	Modificado	Modificado por	Tamaño de arch...	Compartir
 Boletin de seguridad.pdf	20 de noviembre	Alba Graciela Rodríguez	814 KB	 Compartido
 Correo - alerta ante correos electrónicos so...	20 de noviembre	Alba Graciela Rodríguez	1,71 MB	 Compartido
 Correo Reporta incidentes de seguridad!.pdf	20 de noviembre	Alba Graciela Rodríguez	1,07 MB	 Compartido
 Correo_ Boletín de seguridad Ago23.pdf	20 de noviembre	Alba Graciela Rodríguez	123 KB	 Compartido
 Sesión capacitación politicas ...	20 de noviembre	Alba Graciela Rodríguez	334 KB	 Compartido

Fuente: imagen de drive compartido para información compartida en la auditoría.

Al revisar estos documentos, no permiten dar cuenta de lo registrado en el campo "Observación medición"; dado que no se pudo validar las actividades allí descritas.

Actividades relacionadas en el PETI finalizadas dentro de las fechas programadas dando cumplimiento a los lineamientos y estándares establecidos en las Políticas de Gobierno y Seguridad Digital, de acuerdo con las directrices emitidas por MinTIC

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
05/oct./2023	90	58	58	90	80	Para el tercer trimestre 2023, se presentó avances la totalidad de las acciones programadas para el periodo 4 de 4 y un avance acumulado de 14,5 entregables de los 25 programados para la vigencia. Teniendo en cuenta lo anterior se estima un avance del 58%. Durante este trimestre se dieron por terminadas (100%) las siguientes actividades: Hoja de ruta de implementación de seguridad Digital.
07/jul./2023	90	42	42	90	80	Para el segundo trimestre de la Vigencia 2023, el Plan Estratégico de Tecnologías de la Información (PETI-INM) fue actualizado y se establecieron 25 entregables en su Hoja de Ruta para la vigencia; se presentó avances en 10,5 de los 25 productos y/o entregables programados para la vigencia. Teniendo en cuenta lo anterior se estima un avance del 42%. Durante este trimestre se dieron por terminadas (100%) las siguientes tres actividades: Diagnóstico de la arquitectura frente a la seguridad digital, Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co para hora legal, Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co para pagina web. Por otra parte se incumplió la ejecución de la actividad Implementación de un esquema de gobernanza y los procesos asociados para la gestión de TI, esta actividad será ejecutada en el próximo periodo.
10/abr./2023	90	60	60	90	80	Para el primer trimestre de la Vigencia 2023, el Plan Estratégico de Tecnologías de la Información (PETI-INM), en el marco de Hoja de Ruta establecida para la vigencia, presentó avances en seis (06) de los diez (10) productos y/o entregables programados para la vigencia. Teniendo en cuenta lo anterior se estima un avance del 20,5%, para un cumplimiento total del 60%. Durante el tercer trimestre se dieron por terminadas (100%) las siguientes tres actividades: IT-001 Implementación de

						servicio de recaudo PSE para recaudos de servicios del INM, IT-006 Implementar y mantener protocolo IPV6 ampliando su cobertura a todos los dispositivos del INM (Ejecutada en 2022 en su totalidad). Se solicitará modificación del plan para actualización de actividades.
--	--	--	--	--	--	--

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=Mjc2&FechaIni=MjkvMTEvMjAyMg==&FechaFin=MjkvMTEvMjAyMw==>

Mis archivos > Auditoria de OTIC > INDICADORES > 1.8.4. PETI

Nombre	Modificado	Modificado por	Tamaño de arch...	Compartir
1.8.4.1. Hoja de Ruta PETI 2023.xlsx	20 de noviembre	Alba Graciela Rodríguez	475 KB	Compartido

Fuente: imagen de drive compartido para información compartida en la auditoría.

Este indicador está sujeto al seguimiento del PETI, y en revisión se detectó que existen incumplimientos que no han permitido desarrollar los productos programados, es por ello que afecta también el cumplimiento de este indicador; por lo anterior, se recomienda hacer una revisión para dar cumplimiento a los productos programados en el PETI, de esta manera no afectar este indicador.

Canal de datos institucional con una disponibilidad del 99.98% mensual garantizando la disponibilidad y continuidad de los servicios de la entidad y fortaleciendo de manera operativa los procesos organizacionales

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
06/oct./2023	95	99,980551774	99,980551774	95	90	De acuerdo con el reporte mensual del proveedor de servicios de Conectividad e Internet Dedicado se presentó un tiempo total de indisponibilidad de 0,14 horas, lo que se traduce en una disponibilidad del 99,98% en el mes, porcentaje que se encuentra en nivel satisfactorio.
05/sep./2023	95	99,980551774	99,980551774	95	90	De acuerdo con el reporte mensual del proveedor de servicios de Conectividad e Internet Dedicado se presentó un tiempo total de indisponibilidad de 0,14 horas, lo que se traduce en una disponibilidad del 99,98% en el mes, porcentaje que se encuentra en nivel satisfactorio.
08/ago./2023	95	99,980551774	99,980551774	95	90	De acuerdo con el reporte mensual del proveedor de servicios de Conectividad e Internet Dedicado se presentó un tiempo total de indisponibilidad de 0,14

horas, lo que se traduce en una disponibilidad del 99,98% en el mes, porcentaje que se encuentra en nivel satisfactorio

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=Mjkz&FechaIni=MjkvMTEvMjAyMw==&FechaFin=MjkvMTEvMjAyMw==>

Como evidencia se presentó:

Mis archivos > Auditoria de OTIC > INDICADORES > 1.8.2. Disponibilidad y Continuidad Canal ☰

Nombre	Modificado	Modificado por	Tamaño de arch...	Compartir
1.8.2.1. Disponibilidad y continuidad de los ...	20 de noviembre	Alba Graciela Rodríguez	102 KB	Compartido

Fuente: imagen de drive compartido para información compartida en la auditoría.

Se observó en este documento, imágenes de correos electrónicos con el porcentaje de disponibilidad del servicio de conectividad para los meses de julio y agosto; pero esta información no fue detallada en los reportes de seguimiento para constatar las cifras.

Incidentes y Requerimientos de TI resueltos dentro de los tiempos establecidos en los Acuerdos de Nivel de Servicio (ANS) buscando la mejora continua en la gestión de TI y una mayor productividad de la entidad

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
13/oct./2023	85	86,6828087167	86,6828087167	85	60	Se registraron durante el mes de septiembre 826 solicitudes en la herramienta GLPI, de los cuales 716 se atendieron dentro de los ANS y 110 por fuera de los tiempos. Para este periodo se obtiene un aumento en el cumplimiento de la meta del indicador, se obtuvo un 87%, porcentaje en nivel satisfactorio. En el periodo se evidencia el aumento de casos con los sistemas de información institucional, esto debido a las actualizaciones que se están ejecutando.
07/sep./2023	85	86,0566448802	86,0566448802	85	60	Se registraron durante el mes de agosto 918 solicitudes en la herramienta GLPI, de los cuales 790 se atendieron dentro de los ANS y 127 por fuera de los tiempos. Para este periodo se obtiene una disminución en el cumplimiento de la meta del indicador, sin embargo, se

						obtuvo un 86%, porcentaje en nivel satisfactorio. Lo anterior se debe a que en agosto se dió prioridad a la migración de las cuentas de correo a microsoft, prestando asistencia a los usuarios, por lo tanto, esto afecto el cumplimiento de los tiempos en otras categorías.
08/ago./2023	85	87,5192604006	87,5192604006	85	60	Se registraron durante el mes de julio 649 solicitudes en la herramienta GLPI, de los cuales 568 se atendieron dentro de los ANS y 81 por fuera de los tiempos. Para este periodo se obtiene un aumento en el cumplimiento de la meta del indicador, atendiendo a que se inició la implementación de los nuevos ANS establecidos en el procedimiento de incidentes y requerimientos de TI. De acuerdo a lo anterior, se obtuvo un cumplimiento del indicador del 88%, porcentaje en nivel satisfactorio.

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=MjU3&FechaIni=MjkwMTEvMjAyMg==>

Como evidencia se aportó:

Mis archivos > Auditoria de OTIC > INDICADORES > 1.8.3. Incidentes y requerimientos MA

Nombre	Modificado	Modificado por	Tamaño de arch...	Compartir
1.8.3.1. Informe de Julio mesa de ayuda Juli...	20 de noviembre	Alba Graciela Rodríguez	1,46 MB	Compartido
1.8.3.2. Informe de agosto mesa de ayuda.p...	20 de noviembre	Alba Graciela Rodríguez	1,29 MB	Compartido
1.8.3.3. Informe de septiembre mesa de ayu...	20 de noviembre	Alba Graciela Rodríguez	702 KB	Compartido

Fuente: imagen de drive compartido para información compartida en la auditoría.

Se observó en estos documentos: tres (3) informes de la mesa de ayuda para los meses de julio, agosto y septiembre que dan cuenta de lo reportado en el campo de "Observación medición".

Procesos de medición automatizados de acuerdo con las necesidades de la entidad que permitan la eficiencia y calidad de los procesos de I INM

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
13/oct./2023	90	100	100	90	70	En el desarrollo de las actividades de automatización de mediciones se programaron y desarrollaron las siguientes

						actividades: (1) Recepción de una (1) solicitud, 2309072 (2) Se encuentran en desarrollo cuatro (4) solicitudes, 2208065, 2208066, 2304068, 2304069 (3) Entrega y finalización de una (1) solicitud, 2305070 (4) Realización de taller programación de software libre Python enfocado en la adquisición de datos
05/jul./2023	90	100	100	90	70	Las actividades de automatización de mediciones en el primer trimestre Q2 de 2023 se han desarrollado con normalidad. En el desarrollo de las actividades de automatización de mediciones se programaron y desarrollaron las siguientes actividades: (1) Realización de la gestión para contratación de los contratistas desarrolladores (2) Se dio continuidad en el desarrollo de las solicitudes 2208065 y 2208066 (3) Se realizaron actividades de desarrollo de Termohigrobarometro con características de transformación digital para Metrología (4) Se dio soporte aplicaciones desarrolladas como hora legal premium
05/abr./2023	90	100	100	90	70	Las actividades de automatización de mediciones en el cuarto trimestre Q1 de 2023 se han desarrollado con normalidad. En el desarrollo de las actividades de automatización de mediciones se programaron y desarrollaron las siguientes actividades: 1) contratación de desarrolladores 2) atención de soporte a solicitudes desarrolladas 2203058, 2203056.

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=Mjc3&FechaIni=MjkvMTEvMjAyMw==&FechaFin=MjkvMTEvMjAyMw==>

Como evidencia se aporta:

Compartir Copiar vínculo Descargar Automatizar Organizar

Mis archivos > Auditoría de OTIC > INDICADORES > 1.8.1. Automaización

Nombre	Modificado	Modificado por	Tamaño de arch...	Compartir	Actividad
1.8.1.1. Acta de inicio 2208065.pdf	20 de noviembre	Alba Graciela Rodríguez	258 KB	Compartido	
1.8.1.2. Acta de entrega y finalizacion proy...	20 de noviembre	Alba Graciela Rodríguez	332 KB	Compartido	
1.8.1.3. Acta de inicio 2208066.pdf	20 de noviembre	Alba Graciela Rodríguez	265 KB	Compartido	
1.8.1.4. Acta de inicio 2304068.pdf	20 de noviembre	Alba Graciela Rodríguez	306 KB	Compartido	
1.8.1.5. Acta de inicio 2304069.pdf	20 de noviembre	Alba Graciela Rodríguez	306 KB	Compartido	
1.8.1.6. Acta de inicio 2309072.pdf	20 de noviembre	Alba Graciela Rodríguez	470 KB	Compartido	
1.8.1.7. Listado de asistencia Taller Program...	20 de noviembre	Alba Graciela Rodríguez	886 KB	Compartido	

Fuente: imagen de drive compartido para información compartida en la auditoría.

Estos documentos responden a Actas de Inicio de Proyectos de Automatización de mediciones; y soportan lo registrado en el campo de "Observación medición".

Requerimientos de Desarrollo y Mantenimiento de Software resueltos de acuerdo con las necesidades de arquitectura empresarial del INM garantizando la eficiencia y calidad de los procesos de I INM

Fecha	Meta	Medición	Valor estimado	Límite superior	Límite inferior	Observación medición
13/oct./2023	80	103,2258064516	103,2258064516	80	50	Durante el mes de septiembre de 2023 se atendieron las solicitudes recibidas. Quedan pendientes tres requerimientos que vienen del mes de agosto, los cuales requiere mayores esfuerzos y dedicación de tiempo. El indicador presenta un porcentaje del 103% atendiendo a que se gestionaron requerimientos de meses anteriores que se encontraban en ejecución.
07/sep./2023	80	103,4482758621	103,4482758621	80	50	Durante el mes de agosto de 2023 se atendieron las solicitudes recibidas. Quedan pendientes tres requerimientos que son de largo aliento y requieren de mayor tiempo de dedicación por ser ajustes de fondo. El indicador presenta un porcentaje del 103% atendiendo a que se gestionaron requerimientos de meses anteriores que se encontraban en ejecución.
08/ago./2023	80	93,0555555556	93,0555555556	80	50	Durante el mes de Julio de 2023 se atendieron las solicitudes

						recibidas, quedando cinco pendientes por atender en el período. Obteniendo el 93%, porcentaje que se encuentra en nivel satisfactorio. En cuanto al requerimiento pendiente del mes de junio, este fue solucionado.
--	--	--	--	--	--	---

Fuente: <https://isolucion-produc.inm.local/Isolucion/Medicion/frmIndicadoresBase.aspx?CodIndicador=Mjcz&FechaIni=MjkvMTEvMjAyMg==&FechaFin=MjkvMTEvMjAyMw==>

Como evidencia se aportó:



Fuente: imagen de drive compartido para información compartida en la auditoría.

En estos archivos, se observa el registro de los casos que se han venido atendiendo.

Matriz de Activos de la Información

En el POSI, se validó la matriz de activos de información y se adiciona las siguientes recomendaciones:

- ✚ No se está contemplando como activos de información los servidores de la INM, estos almacenan y salvaguardan toda la información de la operación de entidad; se recomienda ser evaluada y registrada en esta matriz.
- ✚ De igual manera no se contempla ninguno de los equipos de cómputo de la entidad, que igual deben contener información de los servidores públicos y contratistas.
- ✚ El recurso humano se debería evaluar, de esta manera ver hasta qué punto se deba contemplar la memoria institucional, que pueda adquirir algún servidor público y que en el momento de no contar con ese recurso pueda verse afectada la operación del proceso.
- ✚ Continuar constantemente, monitoreando y actualizando los activos de información de la entidad.

PLANES DE MEJORAMIENTO

De acuerdo con el reporte de seguimiento remitido por la jefe de Control Interno, vía correo electrónico de fecha 08/11/2023 a las diferentes dependencias de la INM, se observa que aún el proceso cuenta con 81 acciones en las que no se ha generado el registro de cierre, además corresponden a las siguientes vigencias:

2017	2019	2020	2021	2022
9	12	24	25	11

Fuente: Archivo "ANEXO_CONSOLIDADO_PLANES_20230930.xlsx"

Por lo anterior, se recomienda generar acciones de manera oportuna para dar cumplimiento a las acciones que desde la vigencia 2017 aún se registran como abiertas.

PRINCIPALES SITUACIONES DETECTADAS / RESULTADOS DE LA AUDITORÍA

OBSERVACIÓN N° 1. PRODUCTOS INCUMPLIDOS

Condición: En documentos: "*Manual de Gobierno Digital*", producto de la actividad "*Implementación de un esquema de gobernanza y los procesos asociados para la gestión de TI*", no se observa en el módulo de documentación de ISOLUCIÓN.

Adicional el producto de la actividad: "*Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co de los servicios ofrecidos por la entidad*", se va a replantear, y a la fecha no se ha dado cumplimiento a esta actividad; lo anterior, se observó en revisión del PETI. Ahora, en lo que respecta al resultado de revisión del POSI, en "*Fase de implementación: Actualizar procedimientos de seguridad y manual de políticas seguridad, según resultado del diagnóstico*" no se cumplió en la construcción de todos los documentos allí planteados (ver detalle en seguimiento POSI de este documento); de igual manera ocurre con los indicadores: "% de Documentación del SGSI actualizada", "% de Sensibilizaciones ejecutadas en Seguridad de la Información", "Actividades relacionadas en el PETI finalizadas dentro de las fechas programadas dando cumplimiento a los lineamientos y estándares establecidos en las Políticas de Gobierno y Seguridad Digital, de acuerdo con las directrices emitidas por MinTIC", "Canal de datos institucional con una disponibilidad del 99.98% mensual garantizando la disponibilidad y continuidad de los servicios de la entidad y fortaleciendo de manera operativa los procesos organizacionales"; que no se observó el respectivo cumplimiento a lo programado.

Criterios: Artículo 2. Objetivos del Sistema de Control Interno en su literal b)

Garantizar la eficacia, la eficiencia y economía en todas las operaciones promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional. De Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"

Causa: Incumplimiento en los productos establecidos.

Consecuencias o Efectos: Posibles incumplimientos en las metas/productos/actividades/acciones programadas.

Recomendación: Reprogramar las metas de productos que a consideración no se puedan cumplir, para mitigar los incumplimientos, de otra parte presentar los cambios en productos con su debida sustentación en los tiempos establecidos a la Oficina de Planeación, tal como se evidenció en las actividades del PETI: a) *"Implementación de un esquema de gobernanza y los procesos asociados para la gestión de TI"*; b) *"Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co de los servicios ofrecidos por la entidad"*; así como el cumplimiento de los productos planteados en las actividades del POSI, como lo es en la *"Fase de implementación: Actualizar procedimientos de seguridad y manual de políticas seguridad, según resultado del diagnóstico."*; y dar cumplimiento a las fechas estipulada para el cierre de las acciones en planes de mejora que se encuentran con incumplimientos.

OBSERVACIÓN N° 2. DOCUMENTOS SIG

Condición: Construcción de documentos o evidencia incompletos o unidad de criterio en los formatos usados, tal y como se evidenció en documentos: a) *"Diagnostico mejoramiento de la seguridad perimetral"* de la actividad: Mejoramiento de la seguridad perimetral. b) *"7. Matriz página web.xlsx"* de actividad *"Cumplimiento de los requisitos de usabilidad y accesibilidad de gov.co para página web"*; c) *"11. E02F011ModeloInformeV.4m (3) (1).pdf"* de la actividad: Fortalecimiento de los sistemas de información; d) *"14. MSPI INM marzo2023.xlsx"* de la actividad: Diagnóstico de la arquitectura frente a la seguridad digital (actividades están descritas en el PETI); e) *"1.7. E-05-F-005-Inventario-AI-v2.1-2023.xlsx"* (evidencia del POSI), que difiere en la referencia de versión frente a lo publicado en ISOLUCIÓN, f) *"Hacer capacitaciones de concientización en seguridad de la información: boletines y charlas"* (POSI); y de los indicadores: g) *"% de Documentación del SGI actualizada"*; h) *"% de Sensibilizaciones ejecutadas en Seguridad de la Información"*; i) *"Canal de datos institucional con una disponibilidad del 99.98% mensual garantizando la disponibilidad y continuidad de los servicios de la entidad y fortaleciendo de manera operativa los procesos organizacionales"*

Criterios: Artículo 2. *Objetivos del sistema de Control Interno; en su literal f)*

"Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos" de la Ley 87 de 1993.

Causa: Estructuración de documentos incompletos o uso de documentos en versiones diferentes a las publicadas en el sistema ISOLUCIÓN.

Consecuencias o Efectos: Puede llegar a ocasionar no tener clara la necesidad y que se estén adquiriendo soluciones sobredimensionadas o limitadas frente a las necesidades; o no contar con la evidencia completa para el análisis de información o soporte de alguna actividad.

Recomendación: Velar por generar documentos con la información suficiente que permita estructurar las necesidades concretas para apoyar la gestión y misión de lo que se requiere; así como la construcción de evidencia completa y uso de formatos en versiones publicadas en ISOLUCIÓN.

OBSERVACIÓN N° 3.

Condición: Los controles de los riesgos 123, 133, 120,122, 125, 126, 130, 121, 124, 131 en su redacción tienen términos ambiguos o responsabilidades que no deben estar a cargo de los profesionales.

Criterios: Numeral 3.2.2.1 Estructura para la descripción del control de la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas" en su Versión 6.

Causa: Se describen controles con términos ambiguos y algunas responsabilidades que no deben tener los profesionales como es la definición de las políticas.

Consecuencias o Efectos: No contar con controles que den cuenta en su aplicación que están aportando a la no materialización de los riesgos.

Recomendación: Mejorar la redacción de los controles, de tal manera que, al ejecutarlos, el resultado apoye a un efectivo monitoreo y seguimiento de los riesgos; así mismo, es importante fortalecer la construcción de algunas de las evidencias, para dar cuenta efectiva de la ejecución de estos, así monitorear la no materialización de los riesgos. En el caso, de que el control no se encuentre documentado, identificar el instrumento adecuado según su aplicación.

Se aclara que las recomendaciones se generan con el propósito de aportar al mejoramiento continuo de los procesos; se acogen y se implementan, por decisión del líder del proceso.

la Ley 87 de 1993 *“Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones”* en su artículo 12 ... Indica: *“Serán funciones del asesor, coordinador, auditor interno o similar las siguientes: literal k) “Verificar que se implanten las medidas respectivas recomendadas”.*

y en el Artículo 3º.- Características del Control Interno. Son características del Control Interno siguientes:

- a. *“El Sistema de Control Interno forma parte integrante de los sistemas contables, financieros, de planeación, de información y operacionales de la respectiva entidad; y,*
- c. *En cada área de la organización, el funcionario encargado de dirigirla es responsable por el control interno ante su jefe inmediato de acuerdo con los niveles de autoridad establecidos en cada entidad”.*

Por lo anterior, se hace la salvedad que la posible causa identificada por la OCI, fue la evidenciada en el proceso auditor (no es una causa que se deba incluir de manera obligatoria en el plan de mejoramiento a suscribir), no obstante, los responsables de la ejecución de la operación de cada actividad, proyecto, programa o proceso, deberán identificar la causa raíz del hallazgo configurado en esta evaluación, la cual puede ser diferente a la inicialmente identificada.

CONCLUSIONES

El control interno del proceso tiene margen para mejorar, siguiendo las recomendaciones presentadas en este informe. Además, se ha notado que se están implementando los controles definidos en el Anexo A de la norma NTC ISO 27001:2022, lo cual fortalecerá la seguridad de la información. Una vez se integren las recomendaciones señaladas en esta auditoría, se podrá evidenciar un progreso continuo en el proceso, demostrando así un avance hacia la mejora constante.

APROBADO POR:	ELABORADO POR:
Sandra Lucía López Pedreros Jefe Oficina de Control Interno	Ana Yancy Urbano Velasco Contratista