INFORME CONSOLIDADO DEL SISTEMA DE GESTIÓN

DE SEGURIDAD DE LA INFORMACIÓN DNP

OFICINA DE CONTROL INTERNO

Elaboró:

Constanza Cárdenas Aguirre
Rigoberto Andrés Vaca

Revisó: Ricardo Bogotá Camargo, Jefe OCI

Diciembre, 2024

Departamento Nacional de Planeación	**INFORME CONSOLIDADO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DNP**
Fecha: Diciembre del 2024	OFICINA DE CONTROL INTERNO

CONTENIDO

1. PLANIFICACION DE LA AUDITORIA

1.1 AUDITORIA INTERNAS

Para el ciclo de auditorías correspondiente a las vigencias 2024 a 2026, la Oficina de Control Interno – OCI, de acuerdo con su Plan Anual de Auditorias, planificó y ejecutó un total de 30 auditorías internas para la vigencia 2024, con un enfoque integral, lo cual permite verificar el cumplimiento de los requisitos aplicables del Sistema de Gestión de Seguridad de la Información bajo la norma ISO 27001:2013, la Resolución 500 de 2021 y su anexo técnico MSPI, las políticas de Gobierno y Seguridad digital del MIPG y el Manual Operativo de Seguridad de la Información. Para el caso de las vigencias 2025 y 2026 se tiene previsto ejecutar 28 y 34 auditorías internas respectivamente.

Ciclo auditorías	2024	2025	2026	Total
Auditorías Internas	30	28*	34*	92

*Datos preliminares sujetos a modificación

1.2 OBJETIVO

Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información del DNP, en cuanto a su conveniencia, adecuación y eficacia, a través de los resultados generados por las auditorías internas y la efectividad de las APCM formuladas, como un elemento e insumo para la Revisión por la Dirección.

1.3 ALCANCE

El informe comprende los resultados de las auditorías internas, evaluaciones y seguimientos realizados durante la vigencia 2024.

2. EJECUCION DE LA AUDITORIA INTERNA

2.1. RESULTADOS DE HALLAZGOS DE LA AUDITORIA INTERNA – 2024

Como resultado de las auditorías realizadas durante el ciclo 2024 a 2026 al Sistema Integrado de Gestión del Departamento Nacional de Planeación DNP, se presenta a continuación el resultado de los hallazgos según su tipo (No conformidad u Oportunidad de mejora), así:

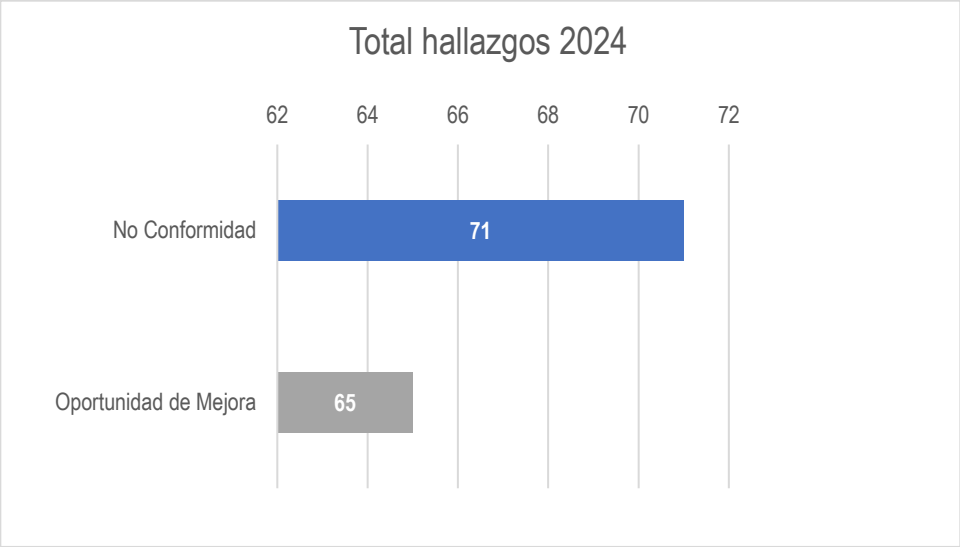
TIPO DE HALLAZGO	2024	2025	2026	TOTAL
No Conformidad	71	-	-	71
Oportunidad de Mejora	65	-	-	65
Total	**136**	**-**	**-**	**136***

TIPO DE HALLAZGO	2024	2025	2026	TOTAL
No Conformidad	52%			52%

Oportunidad de Mejora	48%			48%
Total	**100%**			**100%**

Fuente: Matriz Consolidada de Hallazgos,

*Los 136 hallazgos aquí mencionados corresponden al total de los hallazgos identificados frente a los Sistemas de Gestión de Calidad, Ambiental, Seguridad y Salud en el trabajo, Seguridad de la información. Sistema de Registros y Antisoborno.



Fuente: Matriz Consolidada de Hallazgos

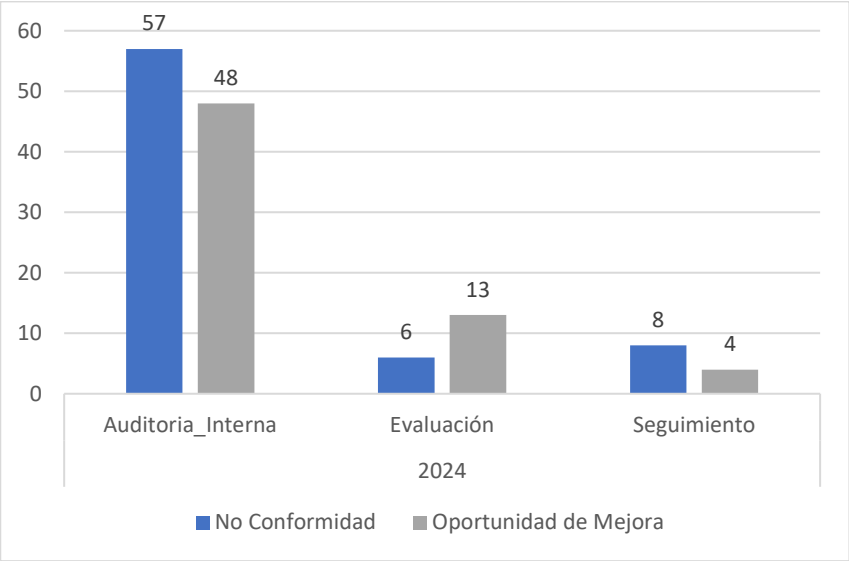
Se observa que durante la vigencia 2024 se identificaron un total de 136 hallazgos, que corresponden a:

- 71 no conformidades, que representan el 52%
- 65 oportunidades de mejora que representan el 48%.

Al revisar la fuente de los hallazgos para la vigencia 2024, se identificó que de los 136, 105 se originaron por auditorías internas, 12 por seguimientos y 19 por evaluaciones.

Fuente	No Conformidad	Oportunidad de Mejora	Total general	%
Auditoría Interna	57	48	105	77%
Evaluación	6	13	19	14%
Seguimiento	8	4	12	9%
Total general	**71**	**65**	**136**	**100%**

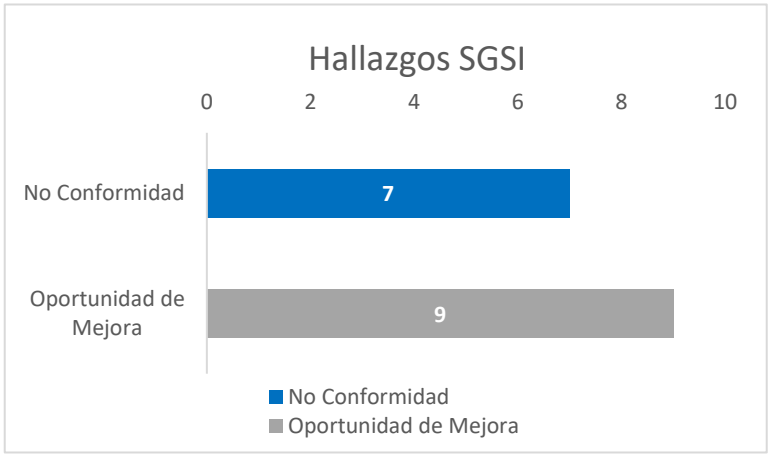
Fuente: Matriz consolidada de hallazgos



Fuente: Matriz Consolidada Hallazgos

De los 136 hallazgos generados en la vigencia 2024, 16 el 12% estuvieron relacionados con la norma ISO 27001:2013 y la Resolución 500 de 2021 con su anexo técnico MSPI así:

Hallazgos	2024	%
No Conformidad	7	**41%**
Oportunidad de Mejora	9	**56%**
Total general	**16**	**100%**

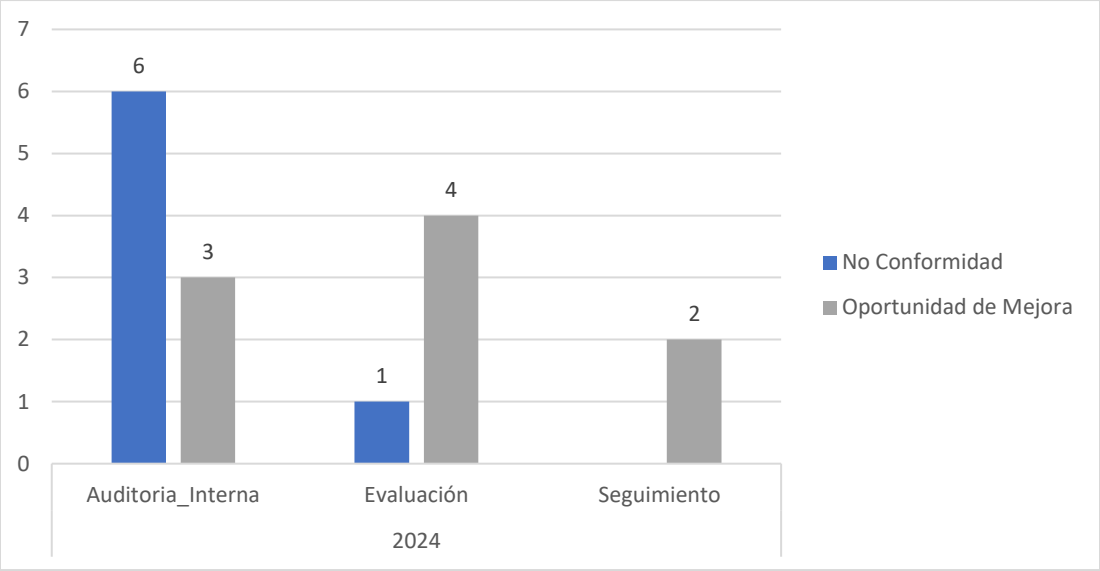


Se observa que durante la vigencia 2024 se identificaron un total de 16 hallazgos relacionados con la norma ISO 27001:2013 y la Resolución 500 de 2021 y su anexo técnico MSPI, que corresponden a:

- 7 no conformidades, que representan el 41%
- 9 oportunidades de mejora que representan el 56%.

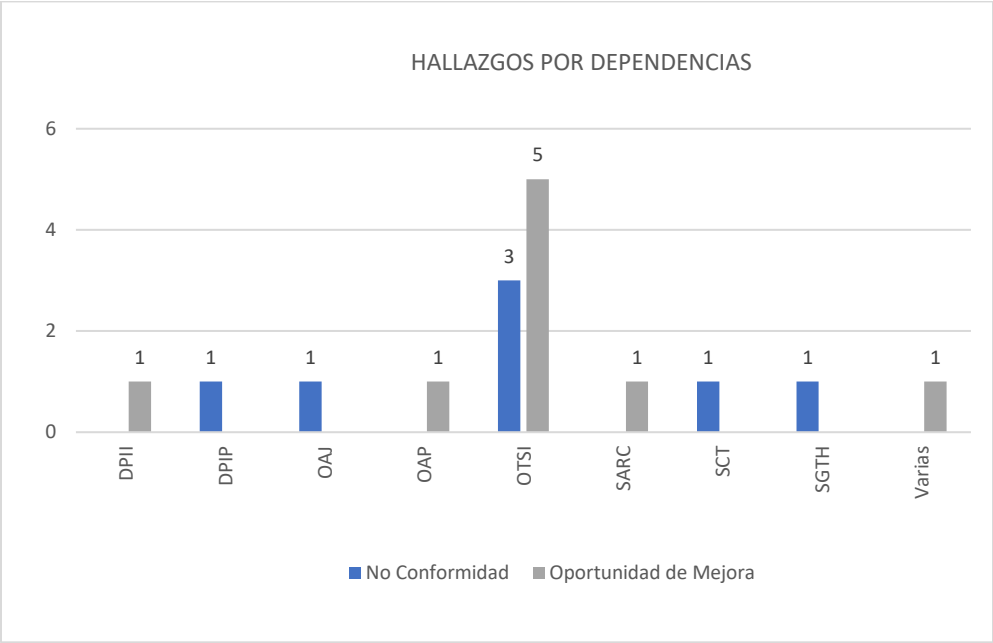
Al revisar la fuente de los hallazgos, se identificó que 9 (56%) se originaron por auditorías internas, 5 (31%) por evaluaciones y 2 (13%) por seguimientos.

Hallazgos	No Conformidad	Oportunidad de Mejora	Total general
2024			
Auditoría Interna	6	3	9
Evaluación	1	4	5
Seguimiento	0	2	2
Total general	**7**	**9**	**16**



Se presenta a continuación las dependencias responsables de la gestión de cada uno de los 17 hallazgos identificados para la vigencia 2024:

Dependencia	No Conformidad	Oportunidad de Mejora	Total general	%
DPII-Dirección de Proyectos e Información para la Inversión		1	1	6%
DPIP-Dirección de Programación de Inversiones Públicas	1		1	6%
OAJ-Oficina Asesora Jurídica	1		1	6%
OAP-Oficina Asesora de Planeación		1	1	6%
OTSI-Oficina de Tecnología y Sistemas de Información	3	5	8	50%
SARC-Subdirección Administrativa y Relacionamiento con la Ciudadanía		1	1	6%
SCT-Subdirección de Contratación	1		1	6%
SGTH-Subdirección de Gestión del Talento Humano	1		1	6%
Varias		1	1	6%
Total general	**7**	**9**	**16**	**100%**



De la gráfica anterior, se observa que para la vigencia 2024 la dependencia con el mayor mejoramiento continuo es la OTSI con un total de 8 que representan el 50% del total, seguido de las demás dependencias (8), cada una con 1 hallazgo (6%).

2.2. RESULTADOS DE HALLAZGOS Vs NUMERALES DE LA ISO 27001:2013

De acuerdo con lo establecido en la **METODOLOGÍA INFORME CONSOLIDADO SISTEMA DE GESTIÓN,** y de acuerdo con el Plan Anual de Auditorias de la vigencia en curso, se debe revisar y actualizar en el Cuadro de Control Procesos Vs Numerales ISO 27001:2013, con los procesos y procedimientos que hacen parte de las auditorías internas, garantizando que durante el ciclo de auditoría del DNP (3 años), se auditen todos los numerales de la norma ISO 27001:2013.

Para el caso de la vigencia 2024, se llevó a cabo la verificación de los 30 procedimientos definidos en el PAA (Plan Anual de Auditoría), definiendo los criterios de la norma a revisar en el desarrollo de los ciclos de auditoría establecidos. (Ver Anexo **CUADRO DE CONTROL PROCESOS Vs NUMERALES ISO 27001:2013 - 2024**).

La distribución de los hallazgos identificados en auditorias, seguimientos y evaluaciones con relación a los requisitos de la norma ISO 27001:2013 y la Resolución 500 de 2021 y su anexo técnico MSPI, reportados durante la vigencia 2024 presentaron los siguientes resultados:

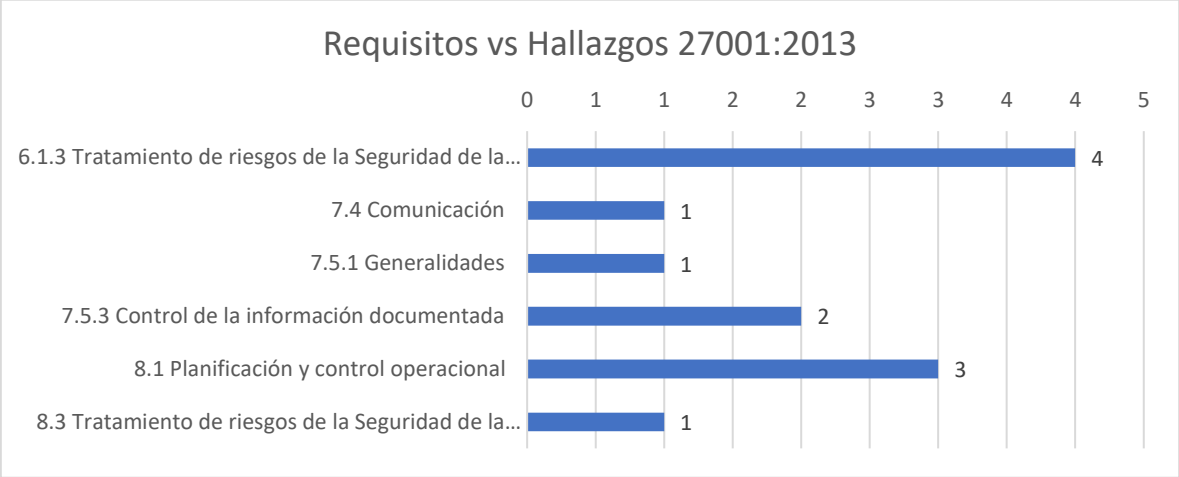
- De los 16 hallazgos se observó que 9 están asociados a 1 criterio y 7 con 2 o más criterios de la norma ISO 27001:

Criterios por hallazgo	No Conformidad	Oportunidad de Mejora	Total general	Criterios
1	3	6	9	9
2 o más criterios	4	3	7	19
Total general	**7**	**9**	**16**	**39**

- Los 39 registros de los 16 hallazgos con 1, 2 o más criterios están relacionados con 6 numerales y 9 controles de la norma ISO 27001:2013 y y la Resolución 500 de 2021, así:

	Vigencia 2024			
Numeral o Anexo Controles NTC ISO 27001:2013	**No Conformidad**	**Oportunidad de mejora**	**Total general**	**%**
6.1.3 Tratamiento de riesgos de la Seguridad de la Información	2	2	4	**33,3%**
7.4 Comunicación	0	1	1	**8,3%**
7.5.1 Generalidades	0	1	1	**8,3%**
7.5.3 Control de la información documentada	0	2	2	**16,7%**
8.1 Planificación y control operacional	1	2	3	**25,0%**
8.3 Tratamiento de riesgos de la Seguridad de la Información	0	1	1	**8,3%**
TOTAL NUMERALES NORMA	**3**	**9**	**12**	**100%**
ANEXO A CONTROLES				
A.6.1 Organización Interna	1	0	**1**	**6,3%**
A.8.1 Responsabilidad por los activos	1	0	**1**	**6,3%**
A.9.1 Requisitos del negocio para control de acceso	1	0	**1**	**6,3%**
A.9.2 Gestión de acceso de usuarios	6	1	**7**	**43,8%**
A.9.3 Responsabilidades de los usuarios	1	0	**1**	**6,3%**
A.9.4 Control de acceso a sistemas y aplicaciones	1	1	**2**	**12,5%**
A.12.1 Procedimientos operacionales y responsabilidades	0	1	**1**	**6,3%**
A.13.2 Transferencia de información	0	1	**1**	**6,3%**
A.18.1 Cumplimiento de requisitos legales y contractuale	1	0	**1**	**6,3%**
TOTALES CONTROLES ANEXO A	**12**	**4**	**16**	**100%**
TOTAL GENERAL	**15**	**13**	**28**	

NUMERALES NORMA



Para los 6 requisitos de la norma ISO 27001:2013 y la Resolución 500 de 2021 con su anexo técnico MSPI, se concluye lo siguiente:

- El requisito *6.1. Acciones para Tratar Riesgos y Oportunidades*, se identificaron un total de 4 hallazgos: 2 No conformidades y 2 Oportunidades de Mejora, lo cual corresponde al 25% del total de los hallazgos relacionados con la norma.

- El requisito *7.5. Información Documentada*, se identificaron un total de 3 Oportunidades de Mejora, lo cual corresponde al 19% del total de los hallazgos relacionados con la norma.

- El requisito *8.1. Planificación y Control Operacional*, se identificaron un total de 3 hallazgos: 1 No conformidad y 2 Oportunidades de Mejora, lo cual corresponde al 19% del total de los hallazgos relacionados con la norma.

- Los demás requisitos con 1 hallazgo (oportunidades mejoras) cada uno, que representa el 6.25%, corresponden a: *7.4 Comunicación*, *7.5.1 Generalidades y 8.3 Tratamiento de Riesgos de la Seguridad de la Información*.

Se concluye que los requisitos 6.1, 7.5 y 8.1, representan el 63% de los hallazgos relacionados con la norma ISO 27001:2013.

ANEXO A - CONTROLES

Fuente: Papel de trabajo

Para 7 objetivos de controles (Anexo A) de la norma ISO 27001:2013 y Resolución 500 con su anexo técnico, se concluye lo siguiente:

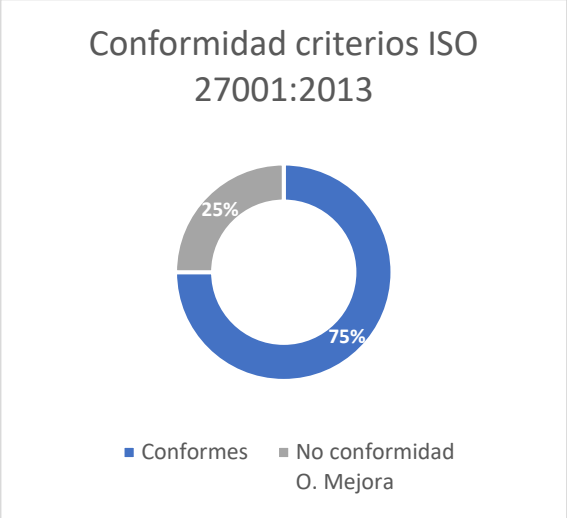
- Para el objetivo de control A 9.2 Gestión de Acceso de Usuarios, se identificaron un total de 7 hallazgos: 6 No conformidades y 1 Oportunidades de Mejora, lo cual corresponde al 44% del total de los hallazgos relacionados con la norma.

- Para el objetivo de control A 9.4. Control de acceso a sistemas y aplicaciones, se identificaron 2 hallazgos (1 No Conformidad y 1 Oportunidad de Mejora), lo cual corresponde al 12.5% del total de los hallazgos relacionados con los objetivos de control de la norma (Anexo A).

- Los demás objetivos de control con 1 hallazgo cada uno, que representa el 6.25%, corresponden a: A6.1 Organización Interna, A8.1 Responsabilidad por los activos, A9.1 Requisitos del negocio para control de acceso, A9.3 Responsabilidades de los usuarios, A12.1 Procedimientos operacionales y responsabilidades, A.13.2 Transferencia de Información y A.18.1 Cumplimiento Requisitos legales y contractuales.

Se concluye que los objetivos de control A9.2 Gestión de acceso de usuarios y A9.4 Control de acceso a sistemas y aplicaciones, representan el 56% de los hallazgos relacionados con los objetivos de control de la norma ISO 27001:2013.

De otro lado, y teniendo en cuenta la ejecución del Plan Anual de Auditoría, cabe resaltar que la conformidad en los numerales no identificados en los hallazgos de las no conformidades y oportunidades de mejora está dada por las conclusiones "conformes", las cuales están alineadas con la estructura de la norma ISO 27001:2013. Así mismo, para la verificación de la conformidad se llevó a cabo el seguimiento en el "Cuadro de Control Procesos Vs Numerales ISO 27001:2013" y el "Anexo 4. Despliegue del Modelo de operación por procesos". Ver detalle en el archivo anexo "Cuadro de control Procesos Vs Numerales ISO27001:2013 – 2024.xls"



Requisitos	56	100%
Conformes	42	75%
No conformidad O. Mejora	14	25%

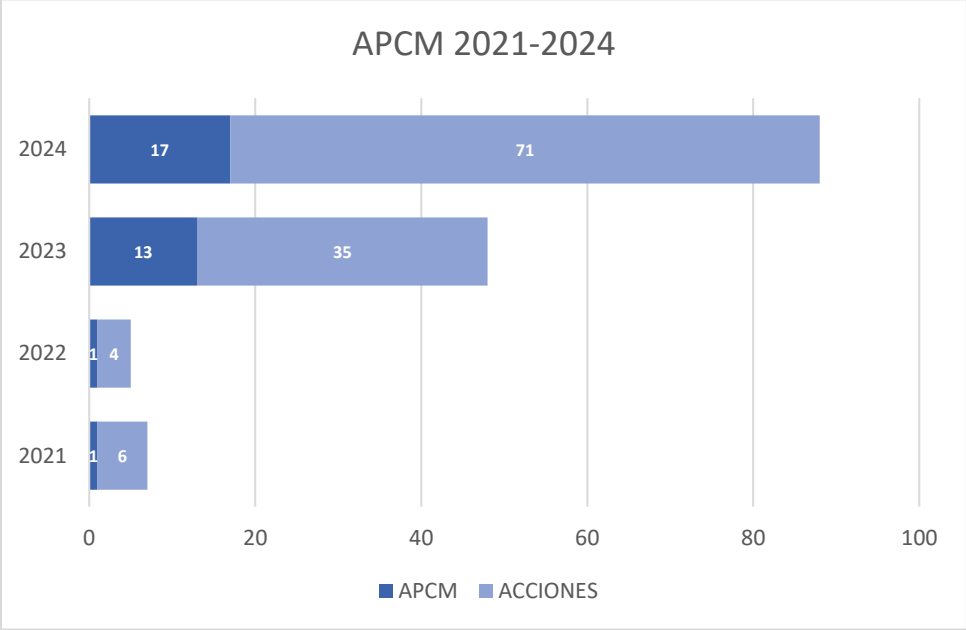
De los 56 requisitos revisados en la norma se observó que a partir de los resultados de las auditorías, seguimientos y evaluación se puede concluir razonablemente conformidad en el 75% de ellos, para el restante 25% las novedades de no conformidad y oportunidad de mejora se detallan en los 15 criterios asociados a los 16 hallazgos identificados.

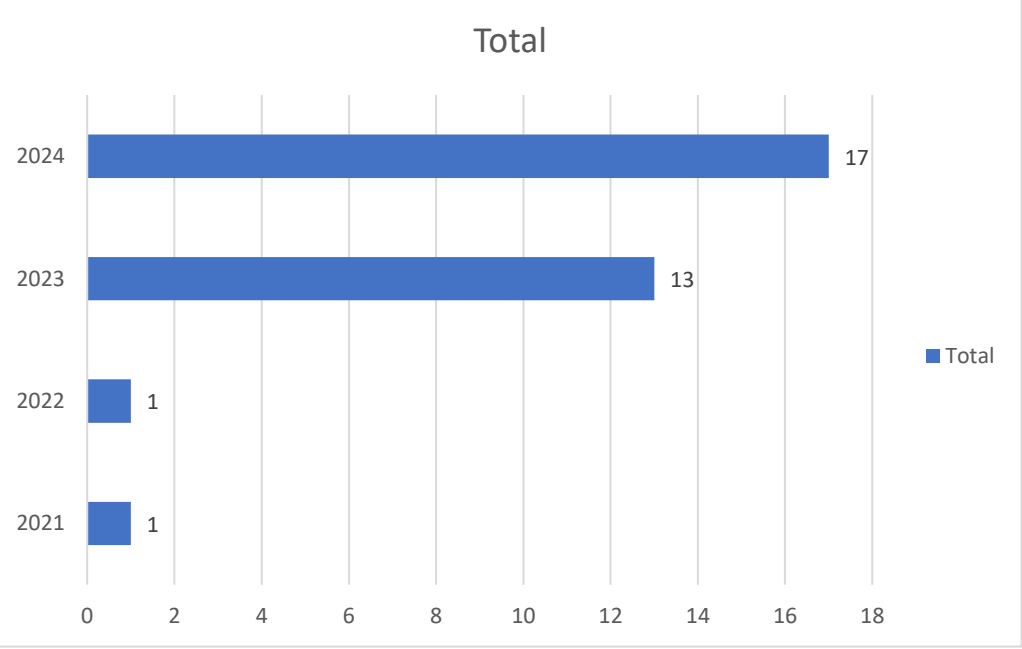
3. ESTADO DE AVANCE LAS APCM

Se presenta el estado de las acciones preventivas, correctivas y de mejora (APCM), desde el 2021 hasta el 30 de noviembre del 2024.

Año	APCM	ACCIONES	% APCM	% ACCIONES
2021	1	6	3%	5%
2022	1	4	3%	3%
2023	13	35	41%	30%
2024	17	71	53%	61%
Total	**32**	**116**	**100%**	**100%**

Fuente: Balance APCM Noviembre 2024.

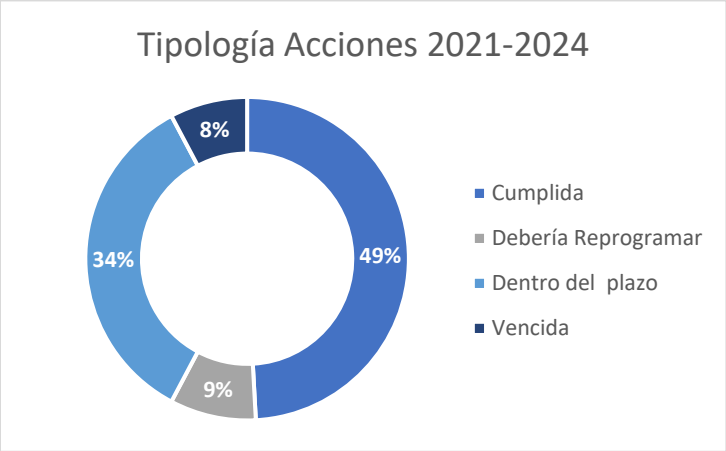

APCM 2021-2024
2024
2023
2022
2021
17
71
13
35
1
4
1
6
0
20
40
60
80
100
APCM
ACCIONES


Total
2024
2023
2022
2021
17
13
1
1
0
2
4
6
8
10
12
14
16
18
Total

Al verificar el comportamiento de las acciones de los dos últimos años al corte para las vigencias 2023 y 2024, se observó que al corte de la vigencia 2023, el 41% (13) de las acciones estaban dentro de los dos últimos años, para el caso de la vigencia 2024, se encontró que el 53% (17) de las acciones estaban dentro de los dos últimos años, por lo anterior se recomienda continuar con el seguimiento oportuno a los planes de mejoramiento.

Estado	2021	2022	2023	2024	Total general	%
Cumplida	5		27	25	57	49%
Debería Reprogramar			4	6	10	9%
Dentro del plazo		2	3	35	40	34%
Vencida	1	2	1	5	9	8%
Total general	**6**	**4**	**35**	**71**	**116**	

Fuente: Balance APCM noviembre 2024.



Según los resultados, se concluye que de 32 APCM formuladas, con corte al 30 de noviembre del 2024, se suscribieron 116 acciones, de las cuales 57 se encuentran con estado “cumplida”, lo cual representa que el 49% de las acciones formuladas, se superaron de manera efectiva; de otro lado, se observó que 40 acciones el 34% se están ejecutando dentro del plazo establecido y se deben fortalecer los controles pues se observa riesgo de incumplimiento en 10 acciones el 9% que se encuentran en estado “Debería reprogramar” y 9 acciones el 8% se encuentran en estado vencido, por lo cual se recomienda tomar las acciones correspondientes para dar cumplimiento en la ejecución de las acciones programadas.

4. CONCLUSIONES GENERALES

Con relación a los resultados obtenidos sobre el Sistema de Gestión de Seguridad de la Información, bajo los criterios establecidos en la norma ISO 27001:2013 y Resolución 500 de 2021 con su anexo técnico,, el Departamento Nacional de Planeación DNP, tiene la capacidad de asegurar el cumplimiento de los requisitos planificados y atender satisfactoriamente al cumplimiento de los objetivos organizacionales; no obstante, es

indispensable que se continue atendiendo los hallazgos de no conformidad y oportunidades de mejora identificados, así como las APCM formuladas, con el objetivo de cumplir de manera efectiva con las necesidades y expectativas de cada parte interesada del Departamento Nacional de Planeación.

De otro lado, en la vigencia 2024 se validaron 56 requisitos de la norma ISO 27001:2013 de los cuales a partir de los resultados de las auditorías, seguimientos y evaluaciones se concluye de manera razonable conformidad en el 75% de ellos y situaciones susceptibles de mejora en el 25%.

Con base en la información de las auditorías, se concluye lo siguiente sobre el Sistema Integrado de Gestión – SIG en referencia del Sistema de Gestión de Seguridad de la Información del Departamento Nacional de Planeación DNP, bajo la norma ISO 27001:2013 y la Resolución 500 con su anexo técnico:

4.1 CONCLUSION EN CUANTO A LA CONVENIENCIA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) es conveniente porque se encuentra articulado con la planificación estratégica, con la política del SGSI, los objetivos estratégicos, apoya el cumplimiento de los requisitos legales, identifica y evalúa los riesgos en Seguridad de la Información y contribuye a establecer y asegurar la confidencialidad, integridad, disponibilidad y la autenticación de la información del DNP y de los sistemas y aplicaciones que la tratan. Sin embargo, se deben fortalecer aquellos aspectos que se consideraron en los hallazgos de la auditoría del MOP y en la evaluación de la Gestión por Dependencias OTSI, auditorias internas, evaluaciones y seguimientos realizados durante la vigencia 2024 haciendo el seguimiento a las APCM formuladas.

4.1. CONCLUSION EN CUANTO A LA ADECUACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

El Sistema de Gestión de Seguridad de la Información es adecuado para dar cumplimiento a los requisitos de la norma ISO 27001:2013 con su anexo de controles, la Resolución 500 de 2021 con su anexo técnico MSPI, los requisitos normativos y reglamentarios establecidos, de igual manera, el Sistema de Gestión de Seguridad de la Información se implementa, se mantiene y se mejora continuamente para el logro de sus resultados previstos y se determina que es capaz de satisfacer los requisitos en materia de seguridad de la información de la norma y/o reglamento aplicable.

4.2. CONCLUSION EN CUANTO A LA EFECTIVIDAD DEL SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION

El Sistema Integrado de Gestión es efectivo, lo que se identifica en la capacidad de lograr la conformidad de los requisitos de SGSI en alineación con su objetivo de gestionar la confidencialidad, integridad y disponibilidad de la información digital de software, hardware, servicios de TI, servicios tecnológicos, servicios de información (aplicativos, portales, sistemas de información) bajo un enfoque tecnológico de seguridad informática de acuerdo con las disposiciones normativas establecidas por las entidades rectoras en la materia y los lineamientos del Sistema Integrado de Gestión (SIG). Sin embargo, se deben fortalecer el seguimiento y

monitoreo por parte de los responsables, a las acciones que se consideraron en los hallazgos de la vigencia 2024 en la auditoría del MOP, en las evaluación de gestión por dependencia de la OTSI y el proyecto de inversión "Fortalecimiento de las TIC para el cumplimiento de los objetivos del DNP a nivel Nacional (Bpin 2022011000029)" , asegurando la mejora continua con la formulación de los planes de mejoramiento para las 7 No Conformidades y 9 Oportunidades de Mejora, relacionadas con: debilidades en el diseño de controles, incumplimiento en la aplicación de políticas de seguridad de la información relacionadas con controles de acceso sobre retiros de permisos de usuarios, uso compartido de usuarios (préstamo de contraseñas), depuración de usuarios, oportunidad en los procesos de contratación de los servicios tecnológicos asociados al Centro de Servicios de Soporte, Conectividad e Internet, entre otros.

Igualmente, es susceptible de mejorar la eficacia y efectividad del Sistema, toda vez que se evidenciaron debilidades en las políticas para la seguridad de la información, matriz de comunicaciones para el componente de SI, gestión integral de los riesgos de TI y actualización oportuna del Manual Operativo de SI, entre otros.

5. RECOMENDACIONES

- Continuar fortaleciendo el proceso de valoración del riesgo que permita determinar los riesgos asociados a la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance, conforme a los reportes cuatrimestrales definidos en el procedimiento de GIR, asegurando que se incluyen el monitoreo continuo de los controles de cada uno de los Sistemas de Información.

- Planificar y monitorear permanentemente las necesidades contractuales asociadas con los servicios tecnológicos, con el fin de asegurar que las contrataciones futuras, se realicen oportunamente en cumplimiento del PAA y los entregables del Plan de Acción y proyectos de inversión, con el fin de mitigar las posibles amenazas y vulnerabilidades que pueden conllevar a la materialización de riesgos en la prestación de los servicios tecnológicos para el DNP.

- Seguir fortaleciendo los mecanismos de seguimiento, con el fin de valorar la eficacia, eficiencia y efectividad de los controles del SGSI, el nivel de ejecución de los planes, los resultados de la gestión, con el propósito de detectar desviaciones, identificar tendencias, y establecer acciones de mejoramiento en adherencia con el procedimiento para la formulación y seguimiento de acciones preventivas, correctivas y de mejora.

- Dar continuidad a las actividades de capacitación, sensibilización y/o concientización con respecto a la seguridad y privacidad de la información, en la que todos los colaboradores del DNP estén al tanto de las políticas de seguridad y privacidad de la información, involucrando al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.

- Asegurar que los lideres técnicos y funcionales gestionen la implementación de los controles en los sistemas de información, dando cumplimiento a sus roles y responsabilidades frente a la identificación de los riesgos e implementación y monitoreo de los controles para cada uno de los sistemas de información que administran y gestionan.

- Continuar fortaleciendo las acciones sobre el control de la información documentada como evidencia soporte del monitoreo de riesgos y ejecución del proyecto de inversión, que permita mantener información idónea para su uso, donde y cuando se necesite.

- Continuar fortaleciendo el seguimiento por parte de la primera y segunda línea de defensa, para el cierre de las acciones identificadas como resultado de los hallazgos de no conformidad y oportunidades de mejora identificadas en las auditorías internas, evaluaciones y/o seguimientos para que se logre contar con un cierre efectivo.

- Adoptar las medidas preventivas y de mejora con el fin de asegurar la medición de la gestión del Sistema de Gestión de Seguridad de la Información, considerando no solo los indicadores de resultado (eficacia), sino también aquellos para medir desempeño conforme a lo definido en la Política de Planeación institucional de MIPG y al Modelo de Seguridad y Privacidad de la Información MSPI, como son los de eficiencia, efectividad y calidad.

- Dar continuidad al proceso de seguimiento y monitoreo que permitan finalizar la gestión de registro de software en la Dirección Nacional de Derechos de Autor y en el inventario de la entidad.