INFORME CONSOLIDADO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DNP

OFICINA DE CONTROL INTERNO

Elaboró:

Omar David Noguera Hernandez, Auditor
Constanza Cárdenas Aguirre, Auditor

Revisó: Ricardo Bogotá Camargo, Jefe OCI

Diciembre, 2023

CONTENIDO

1. PLANIFICACION DE LA AUDITORIA

1.1 AUDITORIAS INTERNAS

Para el ciclo de auditorías correspondiente a las vigencias 2021 a 2023, la Oficina de Control Interno – OCI, de acuerdo con su Plan Anual de Auditorias, planificó y ejecutó un total de 85 auditorías internas, con un enfoque integral, el cual permitió 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.

Ciclo auditorías	2021	2022	2023	Total
Auditorías Internas	27	29	29	85

1.2 OBJETIVO

Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información del DNP, en cuanto a su Confidencialidad, Integridad y Disponibilidad de la información, a través de los resultados generados por las auditorías internas y la eficacia 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 las vigencias 2021, 2022 y 2023.

2. EJECUCION DE LA AUDITORIA INTERNA

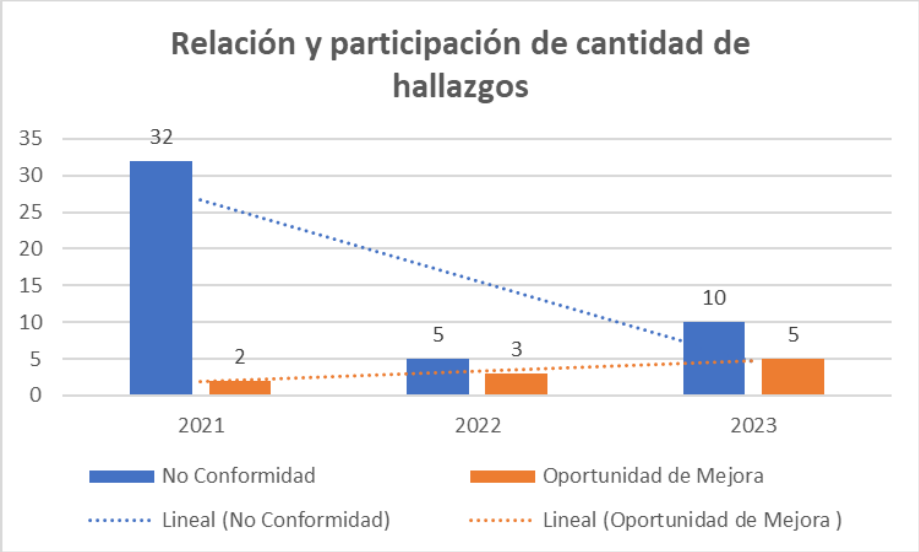
2.1. RESULTADOS DE HALLAZGOS DE LA AUDITORIA INTERNA – 2021 a 2023

Como resultado de las auditorías realizadas durante los ciclos 2021 al 2023 al Sistema de Gestión de Seguridad de la Información, se presenta a continuación el resultado de los hallazgos según su tipo (No conformidad u Oportunidad de Mejora), así:

Relación y participación de cantidad de hallazgos

TIPO DE HALLAZGO	2021	2022	2023	TOTAL
No Conformidad	32	5	10	47
Oportunidad de Mejora	2	3	5	10
Total	**34**	**8**	**15**	**57**

Fuente: Matriz Consolidada de Hallazgos.



Fuente: Matriz Consolidada de Hallazgos

Se observa que durante el periodo 2021 al 2023 se identificó un total de 57 hallazgos, que corresponden a:

- 47 No Conformidades, que representan el 88%
- 10 Oportunidades de Mejora que representan el 12%.

Al comparar las vigencias, las no conformidades disminuyeron en 31%, al pasar de 32 a 10 hallazgos, respecto a las oportunidades de mejora aumentó de 2 a 5 hallazgos.

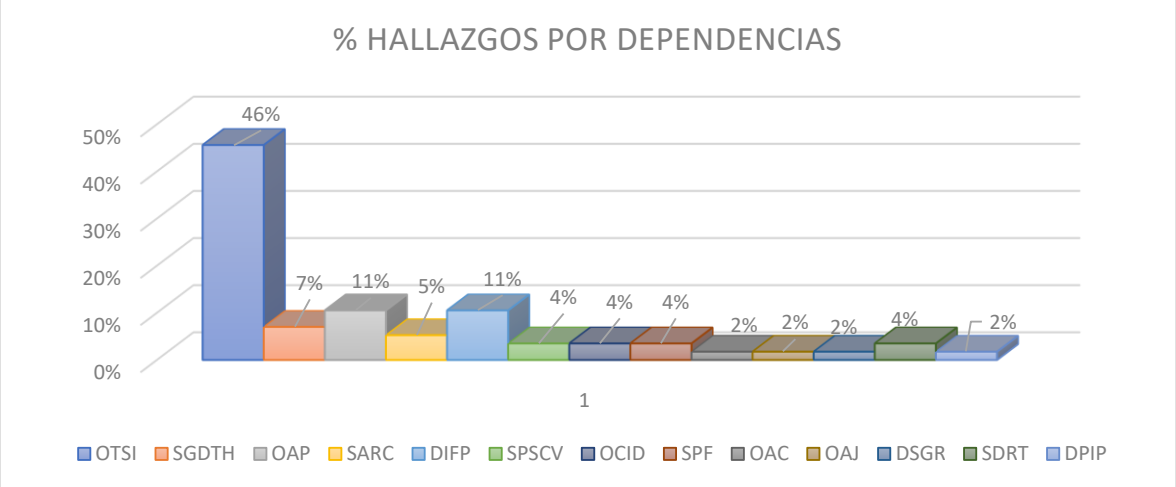
Al revisar la fuente de los hallazgos, se identificó que de los 57 hallazgos todos se originaron por auditorías internas.

Es de aclarar que en la auditoria del Modelo de Operación por Procesos (MOP) se auditaron todos los numerales de la Norma ISO 27001:2013 y sus 114 controles del anexo A y su coherencia con 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.

A continuación se presentan las dependencias responsables de la gestión de cada uno de los 57 hallazgos identificados.

Dependencia	No Conformidad	Oportunidad de Mejora	Total general	%
OTSI-Oficina de Tecnologías y Sistemas de Información	24	2	26	46%
OAP-Oficina Asesora de Planeación	5	1	6	11%
DIFP-Dirección de Inversiones y Finanzas Públicas	4	2	6	11%

Dependencia	No Conformidad	Oportunidad de Mejora	Total general	%
SGDTH-Subdirección de Gestión y Desarrollo del Talento Humano	4	0	4	7%
SA-Subdirección Administrativa	2	1	3	5%
SPSCV-Subdirección de Promoción Social y Calidad de Vida	2	0	2	4%
OCID-Oficina de Control Interno Disciplinario	2	0	2	4%
SPF-Subdirección de Pobreza y Focalización	1	1	2	4%
SDRT-Subdirección de Distribución de Recursos Territoriales	0	2	2	4%
OAC-Oficina Asesora de Comunicaciones	1	0	1	2%
OAJ-Oficina Asesora Jurídica	1	0	1	2%
DSGR-Dirección del Sistema General de Regalías	1	0	1	2%
SGSGR-SUBDIRECCIÓN GENERAL DEL SISTEMA GENERAL DE REGALÍAS	1	1	2	2%
DPIP-Dirección de Programación de Inversiones Públicas	0	1	1	2%
Total general	**47**	**10**	**57**	**100%**



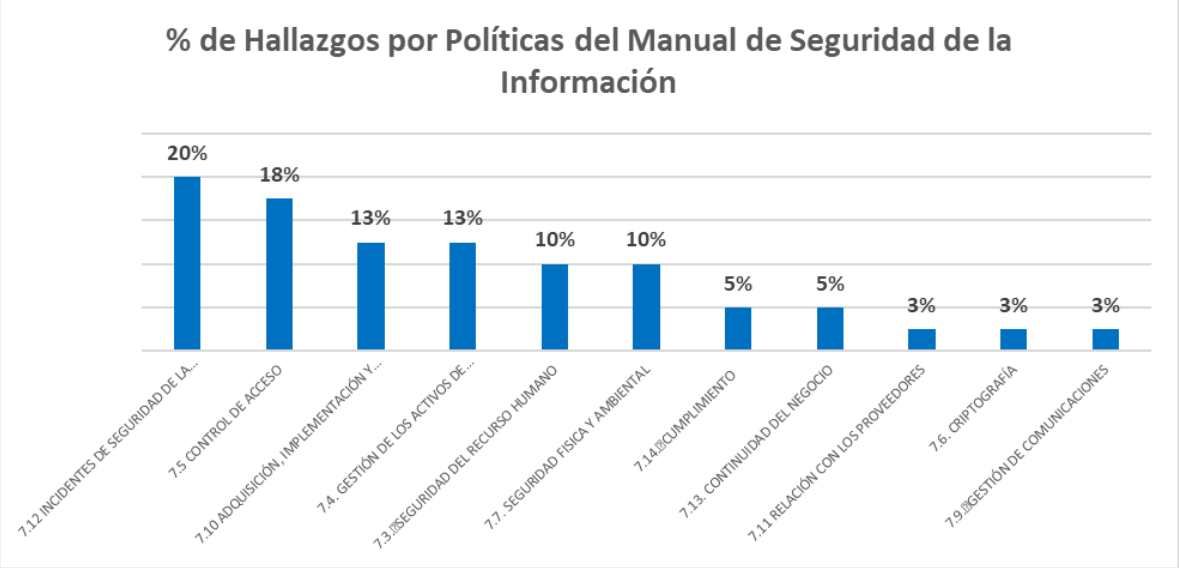
De la gráfica anterior, se observa que las dependencias con el mayor mejoramiento continuo son: la OTSI con un total de 26 que representan el 46% del total, seguido de la OAP con un total de 6 hallazgos con el 11%, luego la DIFP, con 6 hallazgos con el 11%, la SGDTH con 4 hallazgos con el 7%, las SPSCV, OCID, SPF y SDRT cada una con 2 hallazgos con el 4% y OAC, OAJ, DSGR y DPIP cada una con 1 hallazgo con el 2%.

RESULTADOS DE HALLAZGOS Vs POLITICAS DEL MANUAL OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN (M-PG-07 V9)

Se presenta la distribución de los hallazgos identificados en relación con las políticas del M-PG-07 Manual Operativo de Seguridad de la Información V9, reportados durante los periodos del 2021 al 2023. Las Políticas

son las directrices que deben cumplir los usuarios del DNP, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en la información.

Política	Cantidad de Hallazgos	% de Participación
7.12 INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	8	20%
7.5 CONTROL DE ACCESO	7	18%
7.10 ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS	5	13%
7.4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN	5	13%
7.3. SEGURIDAD DEL RECURSO HUMANO	4	10%
7.7. SEGURIDAD FISICA Y AMBIENTAL	4	10%
7.14. CUMPLIMIENTO	2	5%
7.13. CONTINUIDAD DEL NEGOCIO	2	5%
7.11 RELACIÓN CON LOS PROVEEDORES	1	3%
7.6. CRIPTOGRAFÍA	1	3%
7.9. GESTIÓN DE COMUNICACIONES	1	3%



De acuerdo con el resultado se observó lo siguiente:

- **Política, ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**: Esta Política de control representa el 20% de los hallazgos identificados (8 hallazgos). Conforme al análisis realizado se evidenció debilidad en las respuestas a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados y la Resolución 500 de 2021.
- **Política, CONTROL DE ACCESO:** Esta Política de control representa el 18% de los hallazgos identificados (7 hallazgos). Se evidenció debilidad en el acceso no autorizado a sistemas y

aplicaciones y desconocimiento de los usuarios frente al reporte de los incidentes al centro de servicios.

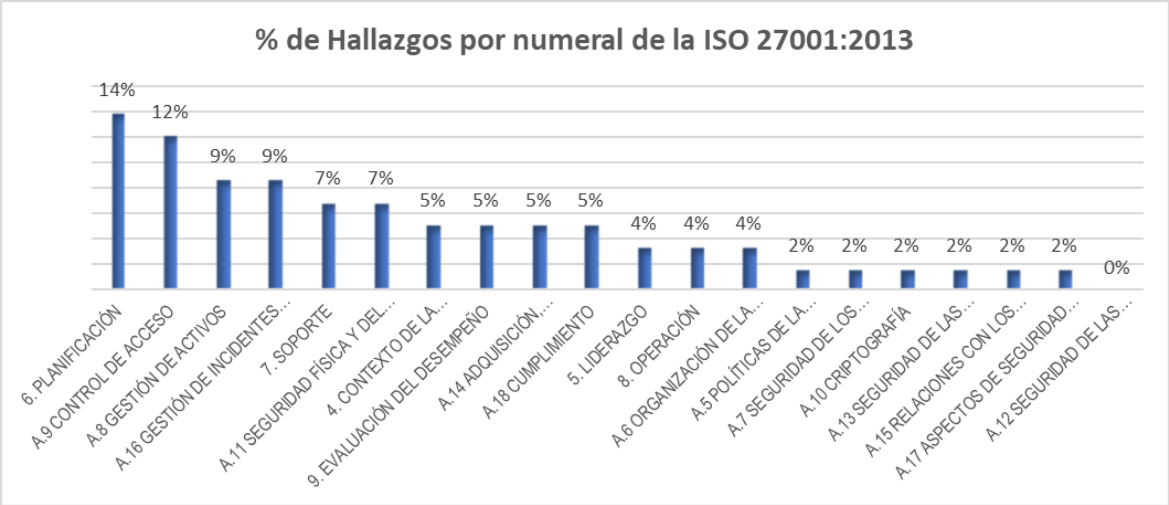
- **Política, ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS:** Esta Política de control representa el 13% de los hallazgos identificados (5 hallazgos). La OTSI definió la Metodología de referencia para la Implementación y Mantenimiento de Sistemas de Información asegurando que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, no obstante, de los 73 sistemas de información del DNP, solamente el 35% (26) cumplen con los requerimientos en cuanto a documentación exigida para su funcionamiento.
- **Política, GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN:** Esta Política de control representa el 13% de los hallazgos identificados (5 hallazgos). Se evidenció que 30 dependencias no realizaron el reporte conforme lo estipulado en el procedimiento, afectando el inventario de activos de información dado que, la no identificación de los activos perjudica la gestión integral de riesgos en cuanto que es un insumo frente a la identificación y análisis de riesgos de seguridad de la información, conforme lo estipula el procedimiento PT-PG-01 GESTION INTEGRAL DE RIESGOS.
- **Política, SEGURIDAD DEL RECURSO HUMANO**: Esta Política de control representa el 10% de los hallazgos identificados (4 hallazgos). Se evidenció incumplimiento en los tiempos de desactivación de los usuarios que terminaron su relación laboral o contractual con la entidad en los sistemas de información del DNP.
- **Política, SEGURIDAD FISICA Y AMBIENTAL:** Esta Política de control representa el 10% de los hallazgos identificados (4 hallazgos). Se evidenciaron debilidades para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información del DNP.
- **Política, CUMPLIMIENTO**: Esta Política de control representa el 5% de los hallazgos identificados (2 hallazgos). Se evidenció debilidad en la identificación de la legislación aplicable, los requisitos contractuales (Normograma), en los registros de derechos de propiedad intelectual de los sistemas de información del DNP y en la privacidad y protección de datos personales debido a que en la página web de la entidad www.dnp.gov.co, se observó base de datos con información sensible de ciudadanos como sexo, discapacidad (salud), grupo de situación especial (comunidad LGBTI) y grupo étnico.
- **Política, CONTINUIDAD DEL NEGOCIO:** Esta Política de control representa el 5% de los hallazgos identificados (2 hallazgos). De acuerdo con lo definido en la auditoría realizada en el 2021 el componente de seguridad de la información no contaba con BCP (Bussines Continuity Plan), el cual es el insumo para el DRP (Disaster Recovery Plan) que asegurara la continuidad del negocio.
- **Política, RELACIÓN CON LOS PROVEEDORES**: Esta Política de control representa el 3% de los hallazgos identificados (1 hallazgo). Se evidenció, debilidad en el tratamiento de la seguridad dentro de los acuerdos con los proveedores, debido al acceso de un proveedor a un sistema de información del DNP, sin que se realice algún control frente al acceso y la protección de la información.
- **Política, CRIPTOGRAFÍA:** Esta Política de control representa el 3% de los hallazgos identificados (1 hallazgo). Se evidenció, que la entidad no ha implementado una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida, ya que no se evidencia documentación sobre grupo de normas y métodos seguros para diferentes sistemas criptográficos.

- **Política, GESTIÓN DE COMUNICACIONES:** Esta Política de control representa el 3% de los hallazgos identificados (1 hallazgo). Se evidenció, debilidad en el control de acceso a los discos de red.

2.2. CUMPLIMIENTO FRENTE A LA ISO 27001:2013

Se presenta la distribución de los hallazgos identificados en auditorias, seguimientos y evaluaciones con relación a los requisitos de la norma ISO 27001:2013 y su anexo A, reportados durante los periodos 2021,2022 y 2023:

Total, Hallazgos por ISO27001				
Numeral	**No Conformidad**	**Oportunidad de Mejora**	**Total, general**	**% de participación**
4. CONTEXTO DE LA ORGANIZACIÓN	3	0	3	5%
5. LIDERAZGO	2	0	2	4%
6. PLANIFICACIÓN	8	4	12	14%
7. SOPORTE	2	2	4	7%
8. OPERACIÓN	2	0	2	4%
9. EVALUACIÓN DEL DESEMPEÑO	2	1	3	5%
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	1	0	1	2%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	2	0	2	4%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	1	0	1	2%
A.8 GESTIÓN DE ACTIVOS	4	1	5	9%
A.9 CONTROL DE ACCESO	7	0	7	12%
A.10 CRIPTOGRAFÍA	1	0	1	2%
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	4	0	4	7%
A.12 SEGURIDAD DE LAS OPERACIONES	0	0	0	0%
A.13 SEGURIDAD DE LAS COMUNICACIONES	1	0	1	2%
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	2	1	3	5%
A.15 RELACIONES CON LOS PROVEEDORES	1	0	0	2%
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	4	1	5	9%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	1	0	1	2%
A.18 CUMPLIMIENTO	3	0	3	5%
TOTAL	**47**	**10**	**57**	**100%**



Fuente: Papel de trabajo

Numeral Norma / Control Anexo	Temáticas
4. CONTEXTO DE LA ORGANIZACIÓN	• Debilidades en el análisis del Contexto interno y externo realizado por la Entidad frente al Sistema Integrado de Gestión. • Debilidades en la identificación de las partes interesadas pertinentes del Sistema de Gestión Ambiental y Seguridad y Salud en el Trabajo
5. LIDERAZGO	• Debilidades en la definición de la Política Sistema integrado de gestión. • Debilidad en la definición de los objetivos de seguridad de la información
6. PLANIFICACIÓN	• Debilidad en el registro del monitoreo de los riesgos 139, 140 y 170, así como debilidad en el registro de la evidencia del control 169.1 Adicionalmente, no se evidenció el reporte del monitoreo y revisión de los riesgos de seguridad de la información: 198 Hurto de la información (Afecta la confidencialidad), 199 No disponibilidad de la información (Afecta la disponibilidad), 200 Perdida integridad de la información (Afecta la integridad). • Se observó en la descripción de los riesgos de seguridad de la información que aplican a la DIFP, que no se contemplaron los elementos definidos en el Anexo 4 “Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades públicas” del Mintic. • Debilidad en el seguimiento y medición de los Objetivos de Seguridad de la información. • Debilidad en la documentación de los controles de los riesgos de seguridad de información para el aplicativo SISPACTOS. • Debilidad de control de acceso al enlace de consulta del documento de distribución “comunicación de la distribución de los recursos del Sistema General de Participaciones”. • Debilidad de control de acceso al enlace de consulta del documento de distribución “comunicación de la distribución de los recursos del Sistema General de Participaciones”. • Desconocimiento del reporte de los Riesgos de Seguridad de la Información
7. SOPORTE	• Debilidad en el control de documentos del sistema Integrado de Gestión del DNP.

Numeral Norma / Control Anexo	Temáticas
	• Incumplimiento sobre la solicitud del Concepto Técnico a la OTSI, para la contratación de prestación de servicios profesionales de los ingenieros de sistemas del SISBEN IV, que realizan las actividades relacionadas con el Procedimiento "Procesamiento y Consolidación de la Información PT-GI-05". • Debilidad en la formación y experiencia laboral y académica del Líder funcional del sistema de información SEVEN, conforme a la Metodología de referencia para la Implementación y Mantenimiento de Sistemas de Información • Incumplimiento frente a la aplicación de las políticas de Seguridad en el Puesto de trabajo • El aplicativo Sisgestión no genera reportes ni tiene opciones de consulta para obtener la trazabilidad del registro, aprobación y novedades de modificación de los planes de acción; y variación en el resultado de avance de los planes institucionales de mayo y junio de 2023 publicados en el sitio Web de la entidad.
8. OPERACIÓN	• Debilidad en la información documentada de los resultados del tratamiento de los riesgos de la seguridad de la información • Debilidades en la eficacia de los controles 184,2 y 200,3 relacionados con el Sistema de Seguridad de la Información. • Se evidenció, que el líder técnico que soportaba la operación de SISGESTION, finalizó su proceso de contratación, y no se generó y planificó un ejercicio de transferencia del conocimiento al nuevo líder técnico que pudiera mitigar los riesgos de operación de todos los módulos, lo que generó la ocurrencia de los riesgos operacionales 134 Deficiencia en el control a las operaciones presupuestales, 211 Pérdida de conocimiento institucional en labores realizadas por contratistas y 200 Perdida integridad de la información (Afecta la integridad).
9. EVALUACIÓN DEL DESEMPEÑO	• Debilidades en el registro de Revisión por la Dirección • Incumplimiento frente al monitoreo de los Riesgos de sistemas de información • Debilidad en definición de indicadores que no permiten medir el desempeño de seguridad de la información y la eficacia del MSPI
A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	• Se evidenció que el Sistema de Información SISGESTION permitió con un usuario de consulta realizar modificación de información sensible de otro usuario. De igual forma, se observó que no se realiza inactivación de usuarios oportunamente al momento de finalización de la relación laboral o contractual con la entidad.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	• Debilidad en la definición de los Inventarios de Proyectos Tic. • Debilidad en la implementación de medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	• Debilidades en la eficacia de los controles 184,2 y 200,3 relacionados con el Sistema de Seguridad de la Información.
A.8 GESTIÓN DE ACTIVOS	• Debilidad en la actualización y publicación del inventario de activos del DNP. • Debilidad en la actualización de los activos de información publicados en "La Rebeca" • Debilidad en la actualización de los activos de información publicados en "La Rebeca"

Numeral Norma / Control Anexo	Temáticas
	• Falta de identificación del activo de información SISBEN APP en el inventario de activos de información de la SPF • Se observaron equipos de cómputo asignados a excontratistas y usuarios con acceso habilitado para publicar contenido en la página WEB e intranet, incumpliendo las políticas de seguridad de la información de la entidad.
A.9 CONTROL DE ACCESO	• Debilidad en la gestión de contraseñas • Debilidad en el registro y cancelación de usuarios en los sistemas de información del DNP. • Debilidad en los controles de acceso a información clasificada en el Sistema de Gestión Documental ORFEO • Debilidades en el cargue de la información relacionada con la Metodología de referencia para la Implementación y Mantenimiento de Sistemas de Información en los repositorios Devops Server. • De los 3 expedientes de procesos disciplinarios (vigencia 2022) verificados en el SGD – ORFEO, se observó que NO cuentan con limitaciones de acceso para la consulta, lo cual podría afectar la confidencialidad e integridad de la información. • "Debilidad en los controles para el acceso a los discos de red del DNP definidos en el formato F-TI-01 • Cuadro actualización accesos y permisos al disco de red." • Roles de acceso definidos en el sistema de información Sisgestion no alineados con lo definido en el Manual para la Formulación de la Planeación Institucional (M-PG-02 Versión 12)
A.10 CRIPTOGRAFÍA	• Debilidad en la implementación de una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	• Debilidad en cuanto a la custodia de los Archivos Físicos • Debilidad en los controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. • Debilidad en el diseño de procedimientos para trabajo en áreas seguras. • Debilidad en la aplicación de la política de escritorio limpio del DNP
A.12 SEGURIDAD DE LAS OPERACIONES	Sin Hallazgos
A.13 SEGURIDAD DE LAS COMUNICACIONES	• Debilidad en el uso de las herramientas institucionales para la transferencia de información
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	• Debilidad en la actualización del Instrumento Inventario de proyectos Tic • Debilidades en la prestación del servicio de mantenimiento, soporte técnico y actualización del sistema de información SEVEN. • "Incumplimiento del proceso metodológico para cumplir con el ciclo de vida de los sistemas de información, afectando la seguridad de los Sistemas SUCOP Y SISGESTION. • Materialización del riesgo código 199 (No disponibilidad de la información) por los incidentes que afectaron el sistema generando indisponibilidad por doce (12) días."
A.15 RELACIONES CON LOS PROVEEDORES	• Debilidad en los controles para definir el acceso de un tercero a los sistemas de información del DNP
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	• Debilidades en la Gestión y tramite de la Correspondencia en las comunicaciones internas y externas, de conformidad con lo

Numeral Norma / Control Anexo	Temáticas
	establecido en las TRD de las dependencias auditadas y el sistema de gestión documental ORFEO. • Debilidades en la migración de expedientes del Grupo de Financiamiento Territorial • Debilidades en la Gestión de Expedientes de conformidad con lo establecido en las TRD de las dependencias auditadas, el sistema de gestión documental ORFEO y el Manual para la Gestión de Documentos y Administración de Archivo • Revisados los (38) expedientes contractuales de los contratistas asociados a la ejecución de los (7) procedimientos objeto de auditoría, vigencias 2020 y 2021, se observó que no reposan documentos generados en el marco de las etapas precontractual y contractual, evidenciando debilidad en el diseño del control frente al término para la conformación de los expedientes virtuales de estos contratos, lo que podría generar incertidumbre en la disponibilidad de esta información para la consulta. • "Debilidad en el establecimiento de las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de • seguridad de la información."
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	• "Debilidad en el establecimiento de las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información."
A.18 CUMPLIMIENTO	• Debilidades en el seguimiento para la actualización del Normograma del Componente de Seguridad de la Información. • Debilidades en el registro de software patentados Incumplimiento de la política de tratamiento de la información de datos personales en el DNP debido a que en la página web de la entidad www.dnp.gov.co, se evidenció base de datos con información sensible de ciudadanos

De lo anterior se concluye que se llevó a cabo la verificación de los criterios de la norma ISO 27001:2013 y su anexo A, la Resolución 500 de 2021, la Política de Gobierno y Seguridad Digital de MIPG y el Manual Operativo de Seguridad de la Información, en las Auditorías realizadas durante el 2021 y 2023 lo que determina que el DNP ha establecido los controles frente a la implementación de la norma que ayuda a fortalecer el Componente de Seguridad de la Información MIPG, protegiendo la información física y digital, activos de información, infraestructura, servicios de TI y servicios de información (aplicativos, portales y sistemas de información).

La implementación oportuna de las acciones preventivas y correctivas enfocados en la mejora continua del proceso ha permitido implementar controles como:

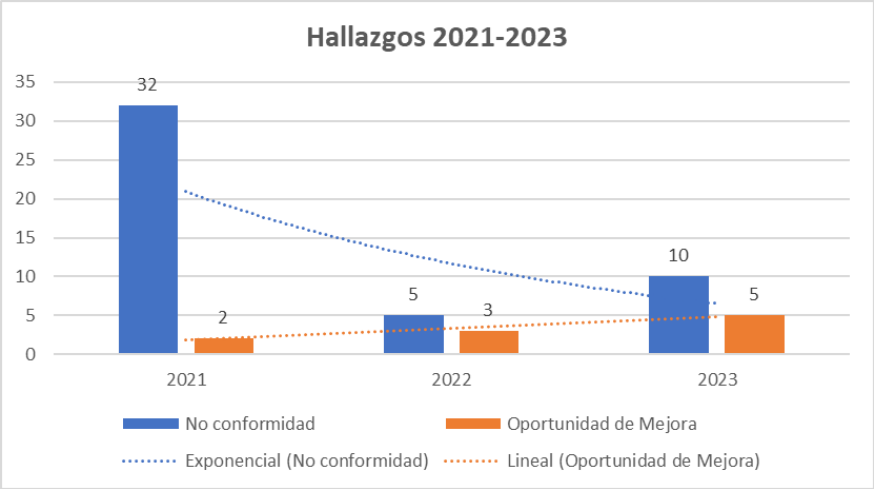
- El establecimiento del contexto interno y externo definido en el Plan Estratégico de Tecnologías de la información PETI.
- La política de la seguridad de la información y los objetivos de la seguridad de la información, alineados con la planeación estratégica del DNP.
- La definición de las acciones para la valoración y tratamiento de los riesgos de seguridad de la información.
- El establecimiento de los recursos para la implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

- La definición de 243 políticas definidas en el Manual Operativo de Seguridad de la información.
- El establecimiento de controles de protección de dispositivos móviles, el trabajo en casa y el teletrabajo.
- La definición de la Metodología de referencia para la Implementación y Mantenimiento de Sistemas de Información.
- Lineamiento para el Desarrollo Seguro de Aplicaciones.
- La construcción del módulo del curso virtual de seguridad de la información que define herramientas de sensibilización.
- La autenticación de doble factor (o autenticación en dos pasos) el cual constituye una medida de seguridad importante que añade una segunda capa de protección a la contraseña asignada.

COMPARATIVO HALLAZGOS CON AUDITORIAS ANTERIORES 2021 – 2023

A continuación, se presenta la variación entre los años 2021 al 2023 donde se refleja una disminución en un 56% (19 hallazgos).

TIPO DE HALLAZGO	2021	2022	Variación 2021-2022	2022	2023	Variación 2022-2023	TOTAL	Variación 2021 a 2023
No Conformidad	32	5	-84%	**5**	10	100%	47	-69%
Oportunidad de Mejora	2	3	50%	**3**	5	67%	10	150%
Total	**34**	**8**	**-76%**	**8**	**15**	**88%**	**57**	**-56%**



Fuente: Matriz Consolidada de hallazgos

- Se observa una disminución de 69% en los hallazgos de No conformidad para el año 2023 en comparación con el año 2021.
- En relación con las Oportunidades de Mejora se observa un incremento para el año 2023 en comparación con el año 2021.

De acuerdo con lo anterior, se observó una disminución de los hallazgos entre el 2021 y 2023 debido a que se han implementado los controles y las recomendaciones definidas en las auditorias y las oportunidades de mejora, los cuales, han generado una mejora frente a la definición de los objetivos específicos y su alineación con la planeación estratégica del DNP, su contexto estratégico, comprendiendo las necesidades y expectativas de las partes interesadas, la determinación del alcance del sistema, las acciones para tratar riesgos y oportunidades introduciendo nuevos conceptos para un análisis sistemático de las amenazas y el establecimiento de acciones para abordar no solo los riesgos sino también las oportunidades que estas plantean, la evaluación del desempeño incluyendo instrumentos de medición (indicadores) que permiten medir la eficacia del sistema, los controles implementados en la seguridad de los trabajadores en teletrabajo fortaleciendo las arquitecturas de seguridad de firewall de red y redes privadas virtuales (VPN), la implementación de la metodología frente al desarrollo y mantenimiento de los sistemas de información implementando controles y procedimientos definidos frente a la seguridad de las operaciones (procedimientos documentados de operación, gestión de cambios, gestión de la capacidad y separación de los ambientes para desarrollo, prueba y operación), la inclusión del certificado de seguridad SSL a los 76 sistemas de información, la alineación de los incidentes de seguridad de la información frente a lo establecido en la Resolución 500 de 2021, los controles definidos en la seguridad física y del entorno, ya que se cuenta con instalaciones con perímetro de seguridad física, controles de acceso físico, seguridad en las oficinas, protección contra amenazas externas y del ambiente, Datacenter con certificado TIER III y áreas de trabajo seguras.

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 2023 así:

Año	APCM	ACCIONES
2021	24	33
2022	12	25
2023	16	22
Total	**52**	**80**

Fuente: Balance APCM noviembre 2023.

Al verificar el comportamiento de las acciones para las vigencias 2021 al 2023, se observó que al corte de la vigencia 2023, se generó dieciséis (16) APCM relacionadas con la Gestión integral de riesgos, la implementación de los indicadores que hacen parte del Modelo de Seguridad y Privacidad de la Información, la anonimización de los datos personales antes de cargarlos en sistemas de información del DNP, la planificación del cambio, el conocimiento de las políticas y metodología para la implementación y mantenimiento de los sistemas de información del DNP y los controles de seguridad de la información para la descarga de software y políticas de escritorio limpio, el acceso a la información, inventario de activos de información, acceso de los usuarios a los sistemas de información, seguridad en los procesos de desarrollo y soporte las cuales se encuentran en proceso de maduración.

Para la vigencia 2022 se generó ocho (8) APCM relacionadas con la Gestión integral de riesgos, el acceso a los códigos fuente de los programas, el acceso a la información y a las funciones de los sistemas de las aplicaciones, inventario de activos de información, suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios, seguridad en los procesos de desarrollo y de soporte y competencia del personal (educación, formación o experiencia)

Para la vigencia 2021 se generaron diecisiete (17) APCM relacionadas con el modelo de gestión integral de riesgos, liderazgo y compromiso, información documentada, Seguridad de la información en la gestión de proyectos, uso aceptable de los activos, política de control de acceso, gestión de llaves, trabajo en áreas seguras, continuidad de seguridad de la información y cumplimiento de requisitos legales y contractuales.

En total se identificaron 52 APCM, las cuales veintinueve (29) que corresponden al 56% están cumplidas, tres (3), el 6% en reprogramación, ocho (8), el 15% están dentro de los plazos establecidos y doce (12), el 23% en estado vencida.

Lo anterior evidencia que se han tomado las acciones para controlar y corregir los hallazgos mediante la formulación y seguimiento de acciones preventivas, correctivas y de mejora, estos seguimientos han permitido mejorar continuamente la conveniencia, adecuación y eficacia del Modelo de Seguridad y Privacidad de la Información.

4. CONCLUSIONES GENERALES

El análisis de los resultados permite evidenciar la implementación y mantenimiento del Sistema de Gestión de Seguridad de la información frente a los requisitos aplicables en la normatividad vigente y su conformidad respecto a la norma ISO 27001:2013 y su anexo A; la Resolución 500 y su anexo técnico MSPI y las políticas de Gobierno y Seguridad Digital, no obstante, es susceptible de mejoramiento continuo en atención a las no conformidades identificadas; esto, con el propósito de fortalecer los controles definidos y prevenir la materialización de riesgos frente al desarrollo de cada una de sus actividades y fortalecimiento de su desempeño, con el objetivo de asegurar de manera efectiva la disponibilidad, integridad y confidencialidad de la información física y virtual.

4.1 CONCLUSION EN CUANTO A LA CONVENIENCIA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

El SGSI es conveniente porque a través de los controles implementados se mitigan los riesgos y se fortalece el desempeño de los procesos, apoyando en el cumplimiento de los requisitos legales, la identificación y evaluación de 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 a través de los sistemas de información, aplicaciones y activos que puedan estar en vulnerabilidad y amenaza.

4.2 CONCLUSION EN CUANTO A LA ADECUACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

El Sistema Integrado de Gestión es adecuado para dar cumplimiento a los requisitos de la norma ISO 27001:2013 y los requisitos normativos y reglamentarios establecidos, desde su Sistema de Seguridad de la

Información, se determina que es capaz de satisfacer los requisitos en materia de seguridad de la información de la norma y/o reglamento aplicable. Sin embargo, 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, inventario de activos, acceso a redes y a servicios en red, suministro de acceso de usuarios y gestión de llaves, entre otros.

4.3 CONCLUSION EN CUANTO A LA EFECTIVIDAD DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN - SGSI

- El Sistema Integrado de Gestión garantiza la mejora, contribuyendo a la implementación y adecuación del SGSI, atendiendo las no conformidades y oportunidades de mejora, evidenciadas para alcanzar el logro de los objetivos institucionales; toda vez que se evidencian 46 hallazgos producto de 18 APCM; 67% (12) están cumplidas y el 33% (6) quedaron abiertas y se recomendó su formulación.

- El Sistema Integrado de Gestión es efectivo, lo que se identifica en la capacidad de lograr la conformidad de los requisitos de SGSI de conformidad con su objetivo 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).

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.

- Fortalecer los mecanismos de capacitación y/o sensibilización para los lideres técnicos y funcionales que aseguren y permitan determinar sus roles y responsabilidades frente a la identificación e implementación de los riesgos y el monitoreo de sus controles para los sistemas de información y así poder minimizar la ocurrencia de los riesgos relacionada con la perdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance de los sistemas de información del DNP.

- Seguir fortaleciendo las actividades que garanticen una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos sus funcionarios 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.

- Fortalecer la aplicación de los controles sobre la planificación del cambio en los sistemas de información del DNP, que puedan afectar el SIG orientando a la entidad, dependencias y procesos hacia el logro de los resultados institucionales y misionales planteados.

- Seguir fortaleciendo los requisitos de accesibilidad que son aplicables a la página web de la Entidad conforme lo establece la (NTC) 5854 que define los requisitos de accesibilidad que son aplicables a las páginas web.

- Adelantar las acciones que permitan fortalecer los controles frente a las Tecnologías de la información y la inteligencia artificial conforme lo establece la Norma ISO 42001:2023 que proporciona directrices sobre la gestión del riesgo al que se enfrentan las organizaciones durante el desarrollo y la aplicación de técnicas y sistemas de inteligencia artificial (IA).

- Implementar lo establecido en el Decreto 1263 de 2022 el cual el DNP utilice tecnologías emergentes de cuarta revolución industrial como la robótica para mejorar la prestación de los servicios de la entidad.

- Adelantar las disposiciones contenidas en la Directiva Presidencial No.15 de marzo de 2021 Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos.

- Establecer la pertinencia de una política frente a la cibercriminalidad, con el propósito de proteger las redes informáticas y los diferentes activos de información del DNP.

- Fortalecer los controles y las capacidades de ciberdefensa con un enfoque de gestión de riesgos y poder definir en la metodología de riesgos las nuevas amenazas y vulnerabilidades cibernéticas.

- Frente al incremento de incidentes de tipo phishing (el phishing es un ataque que intenta robar su dinero o su identidad), seguir fortaleciendo las actividades para que los colaboradores del DNP, puedan identificar correos electrónicos maliciosos que buscan capturar información institucional y/o personal que pueda ocasionar la materialización de riesgos de seguridad de la información como daño, fuga, hurto, no disponibilidad, pérdida de integridad y/o tratamiento inadecuado de los datos abiertos y personales.