INFORME CONSOLIDADO DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN

SGSI

OFICINA DE CONTROL INTERNO

Elaboró: Omar David Noguera Hernández, Auditor

Revisó: Ricardo Bogotá Camargo, Jefe Oficina de Control Interno.

Diciembre, 2022

CONTENIDO

1. PLANIFICACION DE LA AUDITORIA

1.1 AUDITORIA INTERNAS

Para el periodo comprendido en el 2022, la Oficina de Control Interno – OCI, de acuerdo con su Plan Anual de Auditorias, planificó y ejecutó un total de 29 auditorías internas, con un enfoque integral, el cual permitió verificar el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, de acuerdo con el Manual Operativo de Seguridad de la Información V7 del DNP.

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 informes recopilados de todas las auditorías internas realizadas durante 2022, recomendaciones y conclusiones generales.

1.4 INTRODUCCIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) se encuentra articulado con el Sistema Integrado de Gestión, la normatividad de Protección de Datos Personales, Resolución 500 de 2021 con las directrices del Modelo de Seguridad y Privacidad de la Información de Mintic Anexo1 MSPI, el MIPG en su Política de Gobierno y Seguridad Digital y como referencia de consulta la norma ISO 27001:2013.

Es así que el Departamento Nacional de Planeación cuenta con el Manual Operativo de la Gestión de Seguridad de la Información (GSI), cuyo objetivo es *"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).*

El componente de seguridad de la información (GSI) está alineado con la Política del Sistema Integrado de Gestión. Así mismo, el objetivo del GSI se encuentra articulado con el propósito No. 2 de la Política del Sistema Integrado de Gestión definida como: "Gestionar el tratamiento y acceso a la información institucional, el manejo adecuado de los datos abiertos y personales, protegiendo su integridad, disponibilidad y confidencialidad."

La seguridad de la información es el conjunto de medidas y técnicas que utiliza el DNP para controlar y salvaguardar todos los datos (físicos y digitales) que se manejan dentro de la entidad y asegurar que los datos no salgan de los sistemas de información que ha establecido el DNP, preservando la confidencialidad de la información, así como su integridad y disponibilidad; la información es un activo fundamental y cumple un rol

vital en la entidad, por lo que es importante el compromiso de la Alta Dirección en su estrategia de gestión y protección.

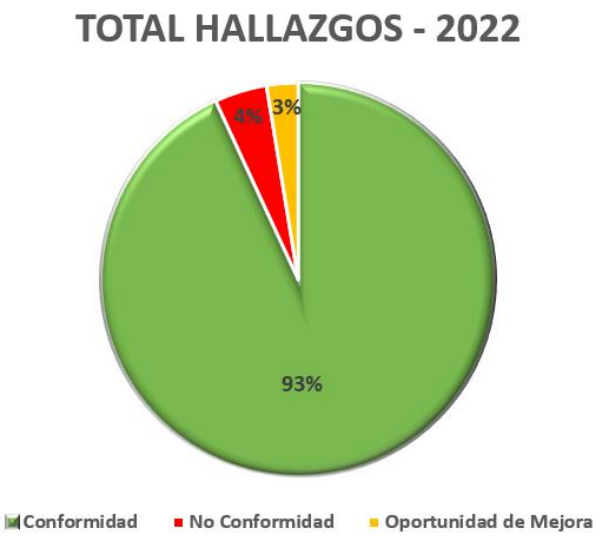
2. EJECUCION DE LAS AUDITORIAS INTERNAS

2.1. RESULTADOS DE HALLAZGOS DE LA AUDITORIA INTERNA – 2022

Durante la vigencia 2022 y en el marco de la ejecución del Plan Anual de Auditorías, evaluaciones y seguimientos, la Oficina de Control Interno realizó verificaciones sobre la aplicabilidad de los criterios de confidencialidad, disponibilidad, integridad, autenticidad y legalidad del Sistema de Gestión de Seguridad de la Información del DNP, con el objetivo de verificar la eficacia en el cumplimiento y la efectividad en la mitigación de los riesgos, de acuerdo con las funciones de las dependencias y/o procesos.

En este informe se presentan los resultados de la evidencia obtenida de acuerdo con los criterios definidos en las auditorías internas realizadas durante la vigencia 2022, los cuales se refieren sólo a las muestras seleccionadas, los registros y/o documentos examinados, no se hacen extensibles como conclusión general del estado de los procesos, teniendo en cuenta que son auditorias selectivas:

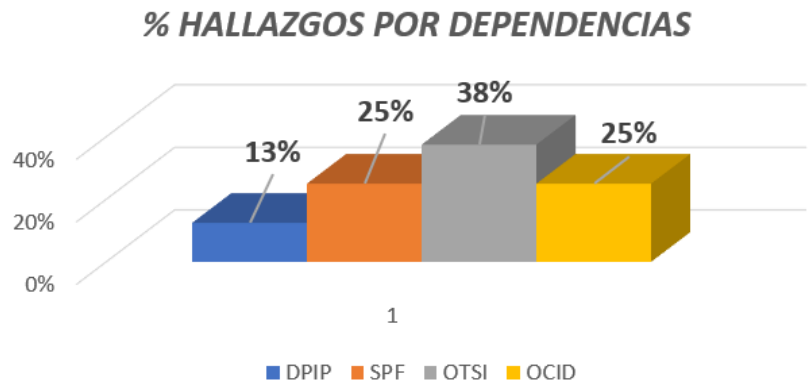
TIPO DE HALLAZGO	TOTAL
Conformidad	108
No Conformidad	5
Oportunidad de Mejora	3
Total, general	**116**



Se observa que durante el periodo 2022 se identificó un total de 8 hallazgos, que corresponden a, 5 hallazgos no conformes, que representan el 4%, 3 oportunidades de mejora que representan el 3% y 108 conformidades que representan el 93% del total de los numerales evaluados en las auditorías que incluyeron el componente de seguridad de la información.
Es de aclarar que para la vigencia 2022 en la auditoria del Modelo de Operación por Procesos (MOP) se auditaron todos los numerales y sus 114 controles de la Norma ISO 27001:2013 y su coherencia con la Resolución 500 de 2021 su anexo técnico MSPI y las políticas de Gobierno y Seguridad digital del MIPG.

Totalizados cada uno de los hallazgos, se presenta a continuación las dependencias responsables de la gestión de cada uno de los hallazgos identificados de acuerdo con la unidad auditable:

Dependencia/Unidad Auditable	No Conformidades	Oportunidad de Mejora	Total, general	% de participación
DPIP-Dirección de Programación de Inversiones Públicas	0	1	1	13%
SPF-Subdirección de Pobreza y Focalización	1	1	1	25%
OTSI-Oficina de Tecnología y Sistemas de Información	2	1	3	38%
OCID-Oficina de Control Interno Disciplinario	2	0	2	25%
Total, general	**5**	**3**	**8**	**100%**



De la gráfica anterior, se observa que las dependencias con el porcentaje de acciones de mejoramiento continuo más alto es la OTSI (Oficina de Tecnología y Sistemas de Información), con 3 hallazgos que representan el 38%, seguida de la OCID (Oficina de Control Interno Disciplinario) y la SPF (Subdirección de Pobreza y Focalización), con 2 hallazgos cada una que representan el 25% y la DPIP (Dirección de Programación de Inversiones Públicas) con 1 hallazgo que representa el 12,5%.

RESULTADOS DE HALLAZGOS Vs POLITICAS DEL MANUAL OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN

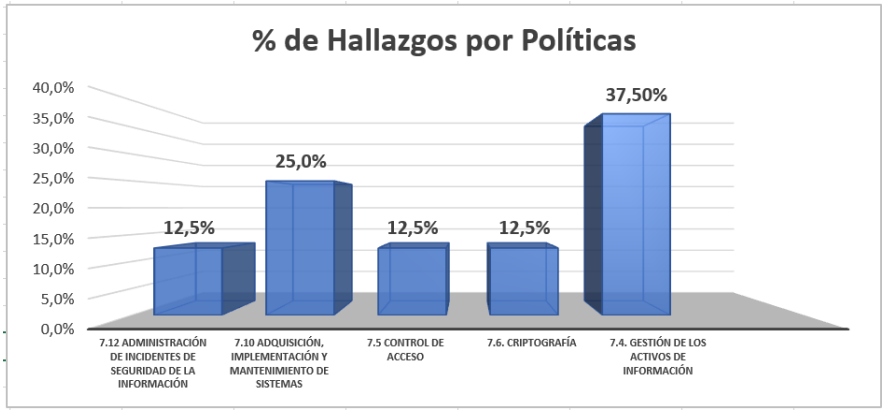
A continuación, se presenta la distribución de los hallazgos identificados en relación con las políticas del Manual Operativo de Seguridad de la Información V7, reportados durante el periodo 2022. Las Políticas son las

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

Objetivos de Control	Políticas Manual Operativo de Seguridad de la Información	No Conformidad	Oportunidad de Mejora	Total, general	%
7.12. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	[PL12-ES1] Las dependencias con el apoyo del Oficina Asesora de Planeación y la Oficina de Tecnología y Sistemas de Información deberá adelantar análisis de riesgos y controles, o actividades relacionadas que permitan valorar y determinar el estado actual de la seguridad de la información, así como los correctivos a que hubiese lugar. La identificación de riesgos de seguridad de la información se realizará de acuerdo el procedimiento PT-PG-01 Gestión integral de riesgos .	0	1	1	12,5%
7.10 ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS	[PL10-ES9] Las dependencias deben solicitar concepto técnico a la Oficina de Tecnología y Sistemas de Información para el aval técnico a la contratación de servicios profesionales de ingenieros de sistemas, electrónicos, software y afines, y el licenciamiento que apoyen el desarrollo o mantenimiento de sistemas de información o plataformas digitales. Es responsabilidad de las dependencias dueñas de los sistemas de información, la asignación de recursos humano, y económico para el mantenimiento, actualización, adquisición de licenciamiento, ya que la Oficina de Tecnología y Sistemas de Información cuenta únicamente con unos recursos específicos ya asignados para el soporte transversal de la plataforma tecnológica, lo cual no incluye nuevos proyectos y/o desarrollos de las dependencias.	1	1	2	25%
7.5. CONTROL DE ACCESO	[PL05-ES1] La identificación de los usuarios ante cada sistema de información será única y confidencial.	1	0	1	12,5%
7.6. CRIPTOGRAFÍA	[PL06-ES1]: Todo sistema de información o servicio tecnológico debe incluir parámetros de seguridad basado en usuarios, perfiles y roles, para ser aplicados en la autorización y autenticación según las necesidades.	1	0	1	12,5%
7.4. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN	[PL04-ES1] La OTSI mantendrá los listados de software incluyendo el Software Específico, Software Free Permitido y No Permitido, los cuales pueden ser consultados en la intranet . En caso de requerir la instalación del software se debe realizar la solicitud a través del Centro de Servicios de acuerdo con el Procedimiento PT-TI-01 Atención a Requerimientos de Servicios TIC , para así validar si el software está autorizado y se cuenta con las licencias disponibles. En caso de requerir un software que no esté incluido en los listados, el usuario deberá gestionar la solicitud con la OTSI, enviando la siguiente información: nombre software, área usuaria, funcionario a quien se asigna la licencia, justificación de uso, aplicación en la entidad, nombre y cargo del solicitante. Nombre y cargo del jefe inmediato que aprueba la solicitud, para su respectivo análisis de viabilidad. La solicitud	2	1	2	37,50%

Objetivos de Control	Políticas Manual Operativo de Seguridad de la Información	No Conformidad	Oportunidad de Mejora	Total, general	%
	no garantiza la asignación del software ya que depende de procesos contractuales, seguridad, pertinencia, entre otros. En los equipos del DNP sólo se podrá instalar y/o utilizar el software autorizado por la OTSI. El software proporcionado por el DNP no puede ser copiado o suministrado a terceros, o instalado en equipos personales de los usuarios.				
	Total General	5	3	8	100%

Las anteriores políticas se consolidan en los siguientes Objetivos de control conforme al Manual Operativo de Seguridad de la Información V7:



De acuerdo con el resultado observado, de los 8 hallazgos identificados, 5 No conformidades y 3 Oportunidades de mejora), se encuentran relacionados con 6 políticas de control del Manual Operativo de Seguridad de la Información; de lo cual se puede concluir:

- **Política, ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**: Esta Política de control representa el 12,5% de los hallazgos identificados (1 hallazgo OM). Conforme al análisis realizado se evidenció debilidad en la documentación de los controles de los riesgos de seguridad de información para el aplicativo SISPACTOS.
- **Política, GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN:** Esta política de Control representa el 35% (3 hallazgos): Se evidencia debilidad en los controles frente a la identificación, clasificación y actualización de los activos de información lo que puede impactar la disponibilidad e integridad de la información, por lo que se deben fortalecer los puntos de control que permitan:
    - Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
    - Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.

- Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.

- **Política CONTROL DE ACCESO:** Esta política representa el 12.5% de los hallazgos (1 NC). Se pudo establecer que los usuarios se les permite acceder a otros discos de red el cual, no se solicitó acceso de acuerdo con lo definido en el formato "F-TI-01 Cuadro accesos y permisos al disco de red", sin control de acceso a sus carpetas y sub carpetas el cual pueden contener información sensible incumpliendo lo estipulado en el control A.9.2.2 Suministro de acceso de usuarios que establece "Se debe implementar un proceso de 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.
- **Política ADQUISICIÓN, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMAS:** Esta política representa el 25% de los hallazgos (2 NC). Se presentaron 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, el cual no permite determinar la documentación que soporta los sistemas de información del DNP como lo son: (documentos concepción de la idea, Solicitud OTSI, Recepción OTSI, Visión y alcance, Análisis y Viabilidad, Plan de trabajo o proyecto entre otros), incumpliendo la metodología del ciclo de vida de los sistemas de información.
- **Política CRIPTOGRAFÍA:** Esta política representa el 12,5% de los hallazgos (1 NC). Se debe garantizar que la entidad continúe fortalecimiento los controles frente al acceso a los sistemas de información (ORFEO), ya que hay expedientes con información sensible el cual no cuentan con las restricciones frente al acceso de la información afectando la confidencialidad e integridad de la información.

2.2. CUMPLIMIENTO FRENTE A LA ISO 27001:2013

A continuación, se presenta el cumplimiento frente a la implementación de la norma y su distribución de los hallazgos identificados en auditorias, seguimientos y evaluaciones con relación a los requisitos de la norma ISO 27001:2013, reportados durante el periodo 2022:

Estado del cumplimiento de requisitos Generales

Numerales	Nombre	Estado
4	Contexto de la organización	Cumple
5	Liderazgo	Cumple
6	Planificación	En proceso de implementación
7	Soporte	Cumple
8	Operación	Cumple
9	Evaluación del desempeño	Cumple
10	Mejora	Cumple

Estado general de implementación ISO 27001 por dominios de su anexo A

# Control	Nombre	Estado
A.5	Política de Seguridad	Cumple
A.6	Aspectos Organizativos de Seguridad de la información	Cumple
A.7	Seguridad de los recursos humanos	Cumple
A.8	Gestión de Activos	En proceso de implementación
A.9	Control de Acceso	En proceso de implementación
A.10	Criptografía	En proceso de implementación
A.11	Seguridad Física	En proceso de implementación
A.12	Seguridad de las Operaciones	Cumple
A.13	Seguridad de las comunicaciones	Cumple
A.14	Adquisición, desarrollo y mantenimiento de sistemas	En proceso de implementación
A.15	Relaciones con los proveedores	Cumple
A.16	Gestión de incidentes de seguridad de la información	Cumple
A.17	Continuidad del negocio	En proceso de implementación
A.18	Cumplimiento	En proceso de implementación

Hallazgos por Numeral.

Total, Hallazgos por ISO27001				
Numeral	**No Conformidad**	**Oportunidad de Mejora**	**Total, general**	**Tema**
6.1.3		1	1	Tratamiento de riesgos de la seguridad de la información
7.2	1		1	Competencia
Total, general	**1**	**1**	**2**	

Hallazgos por Controles Anexo.

Controles	No Conformidad	Oportunidad de Mejora	Total, general	Tema
A.9.4.1	1		1	Restricción de acceso a la información
A.9.4.5	1		1	Control de acceso a códigos fuente de

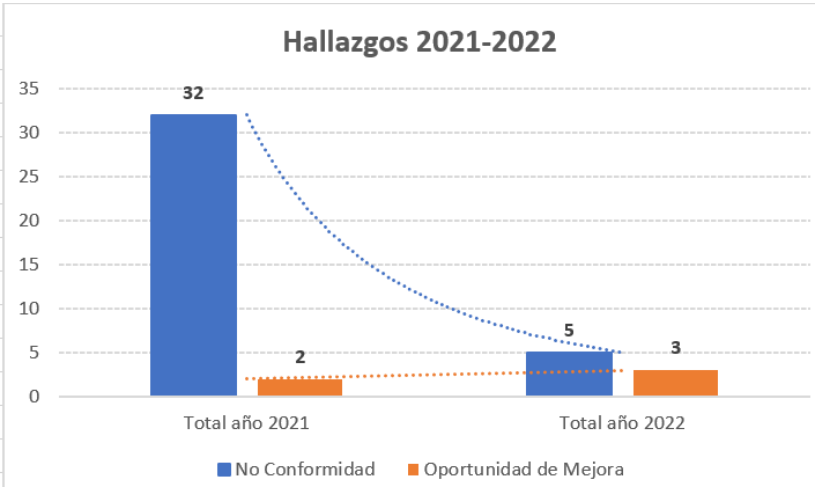
				programas
A.8.1	1	1	2	Inventario de Activos
A.9.2.2	1		1	Suministro de acceso de usuarios
A14.2		1	1	Seguridad en los procesos de desarrollo y de soporte
Total, general	**4**	**2**	**6**	

De acuerdo con los resultados de las auditorías realizadas el cual incluyeron el componente de seguridad de la información se determina que el DNP ha establecido controles frente a la implementación de la norma ISO 27001:2013 que ayuda a fortalecer el Componente de Seguridad de la Información, protegiendo la información física y digital, hardware, 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 la autenticación doble factor, aplicación de accesos con privilegios mínimos, mitigación del riesgo manteniendo las versiones actualizadas (dispositivos, software e infraestructura) y protección de los datos, implementando procedimientos de protección de la información, como la aplicación de etiquetas de confidencialidad y directivas de prevención de perdida de datos.

COMPARATIVO HALLAZGOS CON AUDITORIAS ANTERIORES 2021 – 2022

A continuación, se presenta la variación entre los años 2021 y 2022, donde se refleja una disminución en un 84% (8 hallazgos) de un año a otro.

TIPO DE HALLAZGO	2021	%	2022	%	Diferencia	% de variación	Variación
No Conformidad	32	94%	5	62,5%	-27	-84%	
Oportunidad de Mejora	2	6%	3	37,5%	1	50%	
Total	**34**	**100%**	**8**	**100%**	**-26**	**-76%**	



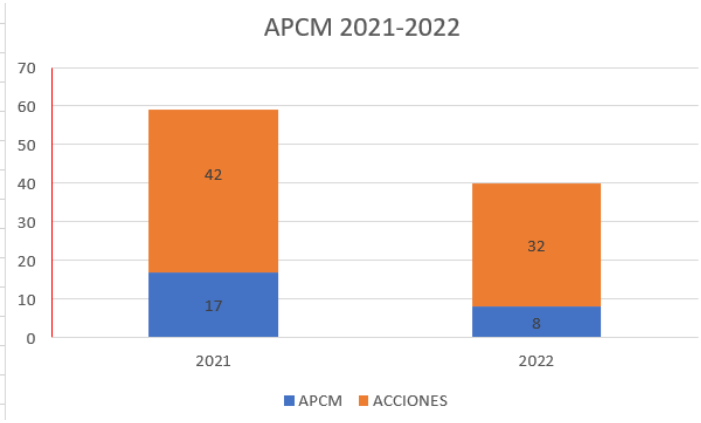
- Se observa una disminución de 26 hallazgos no conformes para el año 2022 en comparación con el año 2021.
- En relación con las oportunidades de mejora se observa un incremento de 1 OM frente al año 2021.

De acuerdo con lo anterior, se observó una disminución de los hallazgos para el 2022 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) aislando y restringiendo el acceso a los recursos y servicios tecnológicos del DNP, 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 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), del 2021 y 2022:

Año	APCM	ACCIONES
2021	17	42
2022	8	32
Total	**25**	**64**



Al verificar el comportamiento de las acciones para las vigencias 2021 y 2022, se observó que al corte de 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, 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 las cuales se encuentran en proceso de maduración. 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 42 acciones, las cuales quince (15) que corresponden al 36% están cumplidas, cuatro (4), el 10% en reprogramación, veintidós (22), el 52% están dentro de los plazos establecidos y una (1), el 2% en estado vencida. Lo anterior, evidencia una disminución del 53% de APCM con relación al 2021, ya que en el 2022 las acciones de mejora han permitido fortalecer los controles definidos frente a lo establecido en la ISO 27001:2013, la resolución 500 de 2021 y la Política de Gobierno y Seguridad digital de MIPG.

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; 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 garantizar de manera efectiva la disponibilidad, integridad y confidencialidad de la información física y virtual.

4.1 CONCLUSION EN CUANTO A LA CONVENENCIA 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 a través de la Metodología de Referencia para la Implementación y Mantenimiento de Sistemas de Información, la implementación de políticas de SI involucrando a todos los funcionarios a su cumplimiento, el contacto con grupos de interés especial de acuerdo con lo establecido en la Resolución 500 de 2021, la seguridad en las comunicaciones, la implementación de la autenticación doble factor fortaleciendo la seguridad a los usuarios en teletrabajo, preservando la confidencialidad, así como su integridad y disponibilidad de los activos de información y el tratamiento para la protección de datos personales.

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

- El Sistema SGSI se encuentra en un proceso de implementación y adecuación de acuerdo con la revisión de todos los numerales de la norma ISO 27001:2013 y los 114 controles definidos en el anexo A, Resolución 500 de 2021 de Mintic y su anexo 1, Política de Gobierno y Seguridad digital, presentando debilidades principalmente en Riesgos y Oportunidades, Propiedad de los activos, Política de control de acceso, Gestión de llaves, Política de escritorio limpio y pantalla limpia, Políticas y procedimientos de transferencia de información, Continuidad de seguridad de la información y el cumplimiento de requisitos legales y contractuales.

- La Entidad mejorará constantemente la eficacia de su Sistema de Gestión de Seguridad de la Información a través de la implementación, aplicación, seguimiento y monitoreo de sus políticas de seguridad de la información, las cuales a través de las auditorías internas se presentaron oportunidades de mejora que deben corresponder a la implementación de las acciones correctivas, preventivas y de mejora.

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

- La Entidad revisa regularmente la eficacia del SGSI, atendiendo al cumplimiento de la norma ISO 27001:2013, Política de Gobierno y Seguridad Digital, la Resolución 500 de Mintic de 2021 y su anexo 1 MSPI, las políticas del Manual Operativo de Seguridad de la Información, los resultados de auditorías de seguridad, incidentes, sugerencias y observaciones de todas las partes implicadas, no obstante es importante desde la segunda línea de defensa (OTSI) se verifique y monitoree continuamente la aplicación efectiva de los controles, y se gestione los riesgos con el propósito de fortalecer la Seguridad de la Información del DNP.

5. RECOMENDACIONES

- Implementar lo establecido en el Decreto 767 de 2022 frente a las nuevas tecnologías que permiten establecer mecanismos frente al uso adecuado, pertinente y eficiente de la tecnología para facilitar el desarrollo de procesos, por lo cual la Política de Gobierno Digital debe integrar a múltiples partes interesadas que actúen mediante instituciones, sedes electrónicas y plataformas afines a la transformación digital.
- 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.
- Fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información Mintic (MSPI) definiendo los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior del DNP un sistema de gestión de seguridad de la información – SGSI y seguridad digital y física, el cual contemple su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar).
- Fortalecer las actividades de capacitación en seguridad de la información que ayude a los empleados a comprender los riesgos que enfrentan el DNP. Esta capacitación debe ser continua y se debe diseñar de una manera que aumente el compromiso, la capacitación de usuarios no es solo una actividad de cumplimiento, sino una parte esencial de la detección y respuesta tempranas ante un ataque, asegurando de que la capacitación que ofrece explique los riesgos en el contexto del trabajo de los empleados y proporcione el contexto y las herramientas que necesitan para entender el comportamiento adecuado, para reconocer ataques e informar actividades inusuales, generando cultura de habilitación, confianza y compromiso mejorando significativamente los informes y brindando advertencias antes de los ataques.
- En consideración al aumento de las amenazas cibernéticas y la especificidad de nuevos delitos, se recomienda fortalecer los controles frente los siguientes ataques principales:
    - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos.
    - La violación de Datos Personales.
    - Acceso abusivo a un sistema informático.
    - Obstaculización ilegítima de sistema informático o red de telecomunicación.
    - Interceptación de datos informáticos.
    - Suplantación de sitios web para capturar datos personales.
    - Uso de software malicioso.
    - Transferencia no consentida de activos de información.
- 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 la parte logística, tecnológica y humana frente a la información que maneja el DNP, con la implementación de controles que fortalezcan y mitiguen la ocurrencia frente a los riesgos identificados de seguridad de la información, ya que el país está en un momento de crisis en términos de ciberataques debido a que se han detectado que el año pasado hubo 41 billones de intentos de ataque y siete billones en Colombia ocupando el tercer puesto en recibir ciberataques en Latinoamérica durante el primer semestre del año, con un total de 6.300 millones. De acuerdo con el Centro Cibernético de la Policía Nacional, hasta octubre de 2022 se registraron 54.121 denuncias por delitos informáticos, esta cifra supera

en 11.223 casos respecto al 2021, al retratar esta cifra desde la Cámara Colombiana de Informática y Telecomunicaciones el aumento fue de 30%.

- 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.
- Fortalecer las acciones sobre el control de cada uno de los Sistemas de Información del DNP, de acuerdo con la Metodología de Referencia para la Implementación y Mantenimiento de Sistemas de Información para que estos cumplan con las características del ciclo de vida de un sistema de información, de conformidad con lo establecido en el Marco de Referencia de Arquitectura TI.