PROCESOS AUDITADOS:	GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN GESTIÓN TECNOLÓGICA.
SECRETARÍAS / DEPENDENCIAS AUDITADAS:	Secretaría de Tecnologías de la información y las Comunicaciones - TIC
AUDITOR LÍDER:	Yuly Andrea Huertas Alonso
AUDITORES:	Ruby Nelcy Romero Hernández Karol Mishelld Tausa García Miguel Baruque Cerquera
AUDITORES ACOMPAÑANTES:	José Patrocinio Quimbay Aguilar
OBJETIVO:	Validar el cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI de acuerdo a lineamientos emitidos por MINTIC, Decreto 338 del 25 de octubre 2018, Artículo 4, con relación al comité de seguridad de la información y las Guías para la gestión de riesgos de activos de información códigos A-GSI-GUI 003 del 14 de junio de 2022 y A-GT-GUI-017 del 21 de mayo del 2019, con el fin de identificar fortalezas y mejoras en los procesos de gestión de seguridad de la información y gestión tecnológica.
ALCANCE:	Del 1 de enero al 31 de octubre de 2022
PERIODO DE LA AUDITORÍA:	2022

TABLA DE CONTENIDO

1 INTRODUCCIÓN Y CONTEXTUALIZACIÓN

En el marco de los lineamientos de la Ley 87 de 1993, “por medio de la cual se establecen normas para el ejercicio del control interno en la entidades y organismos del Estado y se dictan otras disposiciones”, y teniendo en cuenta lo definido en el Modelo Integrado de Planeación y Gestión – MIPG en la dimensión de “Control Interno”, donde se define la auditoría como “*una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la entidad; que ayuda a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno*”.

De acuerdo al rol de evaluación y seguimiento del proceso que lidera la Oficina de Control Interno y en cumplimiento del Plan Anual de Auditorías – V2, aprobado el 14 de junio de 2022 por el Comité Institucional de Control Interno, se ejecuta la auditoría de Seguimiento de la Seguridad de la Información en los procesos de gestión de seguridad de la información y gestión tecnológica, liderados por la Secretaría de Tecnologías de la Información y las Comunicaciones TIC.

Teniendo en cuenta los lineamientos impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones en el marco de la Política de Gobierno Digital establecida en el Decreto 1078 de 2015, Modificada por Decreto 1008 de 2018, en el cual se establecen los componentes, habilitadores transversales, responsables de su implementación y principios de la estrategia de Gobierno Digital, el Decreto 338 del 25 de octubre 2018 y los Controles de Seguridad de la Norma ISO 27001:2013, los cuales garantizan la confidencialidad, integridad y disponibilidad en la entidad.

La Seguridad de la Información uno de los habilitadores transversales de la Política de Gobierno Digital el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, ha definido el Modelo de Seguridad y Privacidad de la Información el cual establece las guías de planeación,

autodiagnóstico, implementación y control del Sistema de Gestión de Seguridad de la Información para entidades Públicas y se articula con las guías de Gestión de riesgos sugeridas por el Departamento Administrativo de la Función Pública - DAFP dentro del marco de la implementación del Modelo Integrado de Planeación y Gestión – MIPG.

2 CRITERIOS DE AUDITORÍA

- Capítulo 1 del Título 9, de la Parte 2, del Libro 2, del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, subrogado por el Decreto 767 del 2022 en el Capítulo 1 sección 2 Artículo 2.2.9.1.2.1 numeral 3.2 . "*Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.*"
- Artículo 4, numeral 4,11 del Decreto 338 del 25 de octubre de 2018.
- Guías para la Gestión de Riesgos de Activos de Información del proceso de Gestión de Seguridad de la Información con código A-GSI-GUI 003 aprobada el 14 de junio de 2022 y del proceso de Gestión Tecnológica con código A-GT-GUI-017 aprobada el 21 de mayo del 2019.
- Norma ISO 27001:2013

3 EVALUACIÓN DE LA GESTIÓN

3.1 EVALUACIÓN DE LOS PROCESOS DE APOYO

3.1.1 Revisar el nivel de madurez del modelo seguridad y privacidad de la información

Para revisar el nivel de madurez modelo seguridad y privacidad de la información se utilizó la herramienta autodiagnóstico denominada “instrumento de identificación de la línea base de seguridad” emitido por MINTIC.

En el ejercicio de evaluación de la auditoría de seguimiento a la seguridad de la información, se realizó la verificación de los controles de la línea base de seguridad administrativa y técnica, manejando como referencia la escala de calificación del instrumento de identificación de la línea base de seguridad “AISI_EA_INSTRUMENTO_EVALUACIÓN_MSPI_01” con un porcentaje de 0 a 100, teniendo en cuenta las evidencias suministradas por la secretaría de TIC a través de correo electrónico el 01/12/2022.

Se evaluaron quince (15) dominios, de los cuales tres (3) se encuentran en inexistente, tres (3) en inicial, tres (3) en repetible y cinco (5) en efectivo, relacionando los resultados de la evaluación por parte de la oficina de control interno:

Evaluación de Efectividad de controles			
No.	**Dominio**	**Calificación Actual**	**Efectividad de control**
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	20	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	58	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50	EFECTIVO

A.8	GESTIÓN DE ACTIVOS	47	EFECTIVO
A.9	CONTROL DE ACCESO	25	REPETIBLE
A.10	CRIPTOGRAFÍA	0	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	7	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	37	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	10	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	40	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	EFECTIVO
A.18	CUMPLIMIENTO	60	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**30**	**REPETIBLE**

En conclusión, para los controles de la línea base de seguridad administrativa se tienen en cuenta los siguientes dominios (A.5, A.6, A.7, A.8, A.15, A.17, A.18), en el cual el dominio con el nivel inicial es la política de seguridad de la información con un cumplimiento del 20% , Se evidencia la política del sistema integral de gestión y control cargada en Isolución E-PID-POL-001 del 26 de marzo de 2020, no contempla los lineamientos de la política de seguridad de la información, ya que debe

incluir objetivos, alcance, debe estar alineada con la estrategia y enfocada a los objetivos de la entidad.

Para los controles de la línea base de seguridad técnica se tienen en cuenta los siguientes dominios (A.9, A.10, A.11, A.12, A.13, A.14, A.16) en los cuales se evidencio que los temas con mayor dificultad son criptografía, adquisición, desarrollo y mantenimiento de sistemas y gestión de incidentes de seguridad de la información teniendo en cuenta que el profesional de la Dirección de Desarrollo Organizacional de la Secretaría de la Función Pública en la reunión realizada el día 30/11/2022 indica que estos controles no han sido implementados, por lo cual en la evaluación se refleja un 0% por otro lado, se evidencio que para el anexo A.13 seguridad de las comunicaciones se tienen un cumplimiento del 10%, para el dominio se están implementado controles como lo es el 5.14 Transferencia de información el cual indica una política sobre las normas, procedimientos y acuerdos para proteger la información en tránsito donde se refleje la clasificación de la información con su respectivo responsable.

para el dominio A.9 Control de acceso se están implementado los controles correspondientes, 5.15 Control de acceso donde se debe implementar una política que especifique lo siguiente: seguridad de las aplicaciones, restricciones al acceso privilegiado, difusión y autorización de la información, segregación de deberes,etc.

Adicionalmente, la Gobernación de Cundinamarca se encuentra actualmente implementado el sistema de gestión de seguridad de la información a través de la meta 377, donde se estableció en un plan de trabajo para la vigencia 2022 en la plataforma Isolución con el objetivo de proteger los activos de información basados en los criterios de disponibilidad, integridad y confidencialidad, sin embargo se observó que para acciones A.6.2.1, A.6.1.4, A.7.1.1 y A.7.1.2 no se ejecutaron en las fechas establecidas, ni se reportó avance de las mismas.

Por otro lado, los controles del anexo A de la norma ISO 27001:2013 A.9, A.10, A.11, A.12, A.13, A.14, A.15, A.16, y A.17 no cuentan con una actividad formulada, es importante tener en cuenta que

para el avance en la implementación se deben ejecutar las acciones planteadas y establecer actividades para los controles faltantes.

3.1.2 Verificar el cumplimiento de las funciones del Comité de seguridad de la información.

Mediante correo electrónico enviado el día 2 de diciembre, el profesional de la dirección de desarrollo Organizacional, indica "*que respecto al punto de la de aprobación de la matriz que se requirió la acta del comité de seguridad de la información se estableció que El Comité Institucional de Gestión y Desempeño, acorde con lo definido en el Decreto 1499 de 2017 debe incluir todos los temas que atiendan la implementación y desarrollo de las políticas de gestión definidas en el MIPG, por lo que aquellos comités que no estén estipulados en una norma específica serán absorbidos por éste.*

Por tal razón ya ha se ha solicitado al Comité Institucional de Gestión y Desempeño que se abra una agenda extraordinaria para poder tocar este tema dar alcance a la implementado en la guía y generar la actualización del formato."

Sin embargo es importante precisar que pese a que el Decreto 1499 de 2017 menciona la integración de los comités, la Gobernación de Cundinamarca mediante Decreto 338 de 2018 se crea y se establecen las obligaciones del comité de Seguridad de la Información, y se incumple el Numeral 4.1 Roles y responsabilidades de la Guía para la Gestión de Riesgos de Activos de Información código A-GSI-GUI-003 aprobada el 14 de junio de 2022, y lo establecido en el acta No. 001 del 09 de octubre de 2019 que tiene como objetivo adoptar el sistema de gestión de la seguridad de la información – SGSI – de la Gobernación de Cundinamarca, en su acuerdo No. Quinto (5) – Sesiones del comité de Seguridad de la información.

3.1.3 Verificación de Cumplimiento Guía para la Gestión de Riesgos de Activos de Información

En cuanto a la gestión de riesgos el proceso de Gestión Tecnológica establece la Guía para la Gestión de Riesgos de Activos de Información con código "A-GT-GUI-017" con fecha de aprobación del 21 de mayo del 2019, la cual es deshabilitada durante la ejecución de la auditoría, teniendo en cuenta que esta misma se actualizo y se asoció al proceso de Gestión de Seguridad de la Información con código A-GSI-GUI-003 aprobada el 14 de junio de 2022 en la herramienta Isolución por parte del líder del proceso.

De la verificación realizada al cumplimiento de la Guía se puede evidenciar lo siguiente:

Frente al numeral No. 4.1 Roles y Responsabilidades se observó que el comité de Seguridad de la Información no ha ejecutado sus roles y responsabilidades establecidas en la Guía para la Gestión de Riesgos de Activos de Información. En cuanto a los roles del Oficial de Seguridad de la Información y Líder del proceso de Seguridad de la Información de la Entidad, se observó que están ejecutando sus actividades.

En cuanto a las fases para la gestión de riesgos establecidas en el numeral No. 6 de la metodología para la Gestión de Riesgos de Activos de Información se evidencia un cumplimiento del 50%, sustentando en el cumplimiento de las siguientes etapas:

- **Establecimiento del contexto**: Se evidenció la elaboración del contexto en el archivo consolidado contexto estratégico (AISI_RNRH_CONT_02 y AISI_RNRH_PART_INT_03)
- **Identificación del riesgo**: Teniendo en cuenta el análisis del contexto estratégico, se realizó la identificación de 712 riesgos en los procesos de Gestión del Bienestar y Desempeño del Talento Humano, Comunicaciones, Gestión de los ingresos, Gestión de Seguridad de la información, Gestión Documental, Gestión Tecnológica y Planificación del Desarrollo Institucional.

- **Análisis del riesgo:** De los riesgos identificados se realizó el análisis de probabilidad de ocurrencia e Impacto en la matriz de gestión de riesgos de seguridad de la información (AISI_RNRH_MAP_CAL_04 y AISI_RNRH_MATRIZ_RG_05).
- **Evaluación del riesgo:** Para cada uno de los riesgos identificados en la primera fase, se realizó la evaluación del riesgo donde se catalogó las diferentes zonas en la matriz de gestión de riesgos de seguridad de la información (AISI_RNRH_MATRIZ_RG_05).

Como resultado de la evaluación de los 712 riesgos identificados, la entidad generará planes de tratamiento solo a 9 riesgos como se menciona en el acta de reunión del día 05/10/2022 (AISI_RNRH_ACTA_RG_05). Es importante tener en cuenta que hacen falta las fases de Tratamiento y control del Riesgo, Seguimiento y calificación a la ejecución de los controles del Riesgo, Monitoreo y Revisión de los Riesgos y Comunicación y Consulta, equivalente al 50% restante de la metodología para la gestión de riesgos.

4 SISTEMA DE CONTROL INTERNO

4.1 EVALUACIÓN DE LOS CRITERIOS DIFERENCIALES DEL SISTEMA DE CONTROL INTERNO

La Oficina de Control interno durante el mes de noviembre llevó a cabo la evaluación de la gestión de riesgos y verificación de cumplimiento de doce (12) criterios diferenciales del Sistema de Control Interno en la primera Línea de Defensa y de acuerdo a las evidencias presentadas el resultado fue el siguiente:

- **Componente Evaluación de Riesgos:** De los cuatro (4) evaluados, cumplen tres (3) relacionados la identificación de cambios, su tratamiento y revisión con la segunda línea de defensa. Sin embargo, la identificación de riesgos de fraude y corrupción no se cumple.
- **Componente Actividades de Control:** De los seis (6) evaluados, cumplen cuatro 4 relacionados con los requerimientos del sistema de control interno, respecto a diseño de controles, seguimiento a riesgos, elaboración de mapa de riesgos de gestión y Dos (2) criterios se cumplen parcialmente, ya que no se han identificado riesgos de corrupción y las evidencias de ejecución de controles están incompletas.
- **Componente Información y Comunicación:** Los dos (2) criterios evaluados cumplen con los requerimientos del sistema de control interno, respecto a generar y comunicar la información relevante, de manera accesible, oportuna, confiable, íntegra y segura, como también frente a la utilización de mecanismos de comunicación definidos por la entidad para interactuar con los grupos de valor.

4.2 EVALUACIÓN DE LA ADMINISTRACIÓN DE LOS RIESGOS

La Oficina de Control interno llevó a cabo la evaluación de gestión de riesgos, durante el mes de noviembre, evaluando los siete (7) controles del proceso de Gestión tecnológica encontrando lo siguiente:

- A nivel de estructura de los riesgos se observó que la redacción cumple con lo establecido en la Guía para la Administración de los Riesgos de Gestión E-PID-GUI-013 numeral 10.2.1.1.5. Descripción del riesgo.
- En cuanto al diseño de controles se obtuvo una calificación MODERADA, debido a que no es claro la definición de un responsable, con cargo y funciones para el seguimiento y ejecución del control, igualmente no se mencionan las acciones a tomar cuando se presenta una desviación que permita la subsanación del evento y/o actividad y que evite materialización del riesgo, es pertinente revisar y aplicar la Guía para la Administración de los Riesgos de

Gestión Código: E-PID-GUI-013 Versión: 8 del 04/04/2022. Por lo anterior se deja un hallazgo de tipo observación.

- En la ejecución de los controles, se pudo evidenciar una calificación MODERADA debido a que no se aportaron de manera oportuna y completa las evidencias solicitadas que permitieran verificar la ejecución de los controles tales como fueron diseñados, dejando como resultado un hallazgo de tipo observación.

5 HALLAZGOS DE AUDITORÍA

5.1 FORTALEZAS

N/A

5.2 OPORTUNIDADES DE MEJORA

- Realizar revisión del contexto y partes interesadas con todos procesos del nivel central de la Gobernación con el fin evidenciar la necesidades actuales de cada uno de estos y expectativas más allá del cumplimiento normativo y/o necesidad identificada.
- Efectuar un análisis más detallado sobre las amenazas y vulnerabilidades identificadas, teniendo en cuenta el contexto y riesgos ya materializados.
- Ejecutar el plan de trabajo en las fechas establecidas.
- Se hace necesario fortalecer conocimientos a funcionarios y contratistas en materia de gestión de riesgos de seguridad digital, política de gobierno digital y el Modelo Integrado de Planeación y Gestión – MIPG.

5.3 OBSERVACIONES

Proceso	Gestión de Tecnológica
Secretaría	Secretaría de Tecnologías de la Información y las Comunicaciones.

Condición: Respecto a las fases para la gestión de riesgos establecidas en el numeral No. 6 de la Guía para la Gestión de Riesgos de Activos de Información se evidencia un avance del 50%, sustentando en el cumplimiento de las siguientes etapas: Establecimiento del contexto, Identificación del riesgo, Análisis del riesgo, Evaluación del riesgo, sin embargo las fases de Tratamiento y control del Riesgo, Seguimiento y calificación a la ejecución de los controles del Riesgo, Monitoreo y Revisión de los Riesgos y Comunicación y Consulta, no se están cumpliendo.

Causa: posibles debilidades en la aplicación de la Guía para la Gestión de Riesgos de Activos de Información, es pertinente hacer el análisis de causas por parte de los líderes de los procesos auditados.

Criterio: Numeral No. 6 de la Guía para la Gestión de Riesgos de Activos de Información código A-GSI-GUI-003 aprobada el 14 de junio de 2022.

Consecuencia: Posible materialización de riesgos de seguridad de la información exponiendo las vulnerabilidades para causar una pérdida o daño en un activo de información.

Evidencia: AISI_RNRH_LISTA_GUIA_RIESGOS_01

5.4 NO CUMPLIMIENTOS

Hallazgo 1

Proceso	Gestión de Tecnológica
Secretaría	Secretaría de Tecnologías de la Información y las Comunicaciones.
Condición: Durante la auditoría interna de gestión y de acuerdo a la solicitud realizada en reunión el día 30 de noviembre, no se allegó acta reunión y/o aprobación de la Guía para gestión de riesgos de Seguridad de la Información por parte del comité de seguridad de la información. **Criterio:** Numeral 4.1 Roles y responsabilidades (Comité de Seguridad de la Información) de la Guía para la Gestión de Riesgos de Activos de Información código A-GSI-GUI-003 aprobada el 14 de junio de 2022 y Acuerdo No. Quinto Sesiones del comité de Seguridad de la información del acta No. 001 del 09 de octubre de 2019. **Causa:** Posibles debilidades en la interpretación de la norma, es pertinente hacer el análisis de causas por parte de los líderes de los procesos auditados. **Consecuencia:** Falta de directrices frente a la operación del sistema que conlleven a posibles materializaciones de riesgos asociados a la seguridad de la información en la Gobernación.	
Evidencia: AISI_RNRH_CORREO_ENT_EVIDEN_06	

Hallazgo 2

Proceso	Gestión de Tecnológica
Secretaría	Secretaría de Tecnologías de la Información y las Comunicaciones.
Condición: En la evaluación realizada se encontraron procedimientos, guías y algunos lineamientos que ya están establecidos, lo que representa el 30% de la efectividad de los controles de la norma ISO 27001:2013 Anexo A y un avance de funcionamiento del modelo de operación	

(PHVA) del 27% dando como resultado un nivel de madurez "**Inicial**" del modelo seguridad y privacidad de la información de acuerdo con la valoración del autodiagnóstico "INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD".

Causa: Debilidades en la Identificación y actualización de requisitos legales, normatividad de Seguridad de la Información y baja apropiación institucional de la Política de Gobierno Digital.

Criterio: Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2).

Consecuencia: Incumplir la responsabilidad de promover la protección y seguridad de la información de nuestros procesos, no garantizando la legalidad, confidencialidad, disponibilidad e integridad de los datos.

Evidencia: AISI_EA_INSTRUMENTO_EVALUACIÓN_MSPI_01

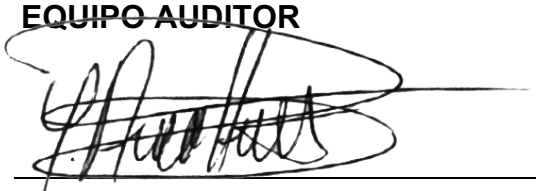
6 CONCLUSIONES DE AUDITORÍA

- Frente a la evaluación de controles del modelo de seguridad y privacidad de la información, se observó un nivel de la efectividad del 30% de implementación de los controles de la norma ISO 27001:2013 Anexo A y un avance de funcionamiento del modelo de operación (PHVA) del 27% dando como resultado un nivel de madurez "**Inicial**", teniendo en cuenta que de los 114 se han implementado 46 controles y 15 se encuentran identificados y asignados a un responsable.
- Es trascendental crear estrategias para la revisión de esta documentación y poder agilizar el trámite ante el sistema de calidad de la entidad acorde a la implementación.
- Es importante validar al interior de la Secretaría frente a los procedimientos vigentes, si toda la documentación del sistema debe ser aprobada por el comité de Seguridad de la información con el fin de facilitar y cumplir oportunamente con los lineamientos emitidos, dado

que durante la vigencia 2022 el comité no se convocó pero si se emitió la Guía para la Gestión de Riesgos de Activos de Información código A-GSI-GUI-003 sin aprobación sin aprobación de dicho comité.

- Frente a la gestión de riesgos es pertinente tomar acciones para la implementación de la Guía para la Gestión de Riesgos de Activos de Información con código A-GSI-GUI-003 aprobada el 14 de junio de 2022 con el fin de mitigar la materialización de riesgos, ya que el nivel de cumplimiento es del 50% para la gestión de riesgos.

EQUIPO AUDITOR



Yuly Andrea Huertas Alonso
Auditor líder

Yoana Marcela Aguirre Torres
Jefe de Oficina de Control Interno

Realizo evaluación con corte a 16 de Diciembre de 2022, por terminación de Contrato

Karol Mishelld Tausa García
Auditor

Realizó evaluación con corte a 16 de Diciembre de 2022, por Vacaciones de acuerdo a Resolución No. 002504 del 25 de Noviembre de 2022

Ruby Nelcy Romero Hernández
Auditor

Realizo evaluación con corte a 27 de Diciembre de 2022, por terminación de Contrato

Miguel Baruque Cerquera
Auditor

Realizó evaluación con corte a 28 de Diciembre de 2022, por terminación del Contrato

José Patrocinio Quimbay Aguilar
Auditor acompañante

FECHA:	**29 de diciembre del 2022**