INFORME DE LEY – CONTROL INTERNO

INFORME DE SEGUIMIENTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) EN LA ANCP – CCE
A CORTE 31 OCTUBRE 2025

La Asesora Experta con Funciones de Control Interno juntamente con su equipo de trabajo, en cumplimiento a lo establecido en la **Ley 87 de 1993** "***Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones",*** así como del **Decreto 648 de 2017** y de conformidad con:

Ley 1581 de 2012 "***Por la cual se dictan disposiciones generales para la protección de datos personales.".***

Ley 1712 de 2014, "***Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.".***

Decreto 1078 de 2015 " ***Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.***" y se compila, entre otros, los Decretos: i) 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital; y, ii) lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Decreto 1083 de 2015 ***"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública."*** y se compila, entre otros, los Decretos: 1499 de 2017: Sistema de Gestión establecido en el Artículo 133 de la Ley 1753 de 2015; 612 de 2018: Integración de los planes institucionales y estratégicos al plan de acción.

Resolución 500 de 2021 (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES), "***Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital."***

Resolución 02277 de 2025 del Ministerio TIC de Colombia actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) que guía a las entidades públicas en la gestión del riesgo digital. Esta resolución actualiza el Anexo 1 de la Resolución 500 de 2021, alineándola con el estándar internacional ISO/IEC 27001:2022 y fortaleciendo la estrategia de seguridad digital del país.

CONPES 3995 de 2020 "***POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL"***

ISO 27001:2022 – Sistema de Gestión de Seguridad de la Información. Estándar internacional que contiene los requisitos para la implementación de un sistema de gestión de seguridad de la información.

INFORME DE LEY – CONTROL INTERNO

ISO 27001:2022 - Anexo A y la ISO 27002:2022. Documento normativo que sirve como guía para implementar los controles de seguridad de la información específicos de la ISO 27000.

En cumplimiento de lo dispuesto en el Plan Anual de Auditorías Basadas en Riesgos 2025, de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, se presenta el Informe De Seguimiento al Modelo De Seguridad Y Privacidad De La Información (MSPI) en la ANCP – CCE a corte 31 octubre 2025. El cual se detalla en el marco del ejercicio auditor evaluando la implementación de los controles de seguridad y privacidad de la información, la revisión de políticas normativas, la gestión de riesgos y la eficacia del modelo según MINTIC. Los resultados obtenidos se detallan en los literales a) y b) del presente informe.

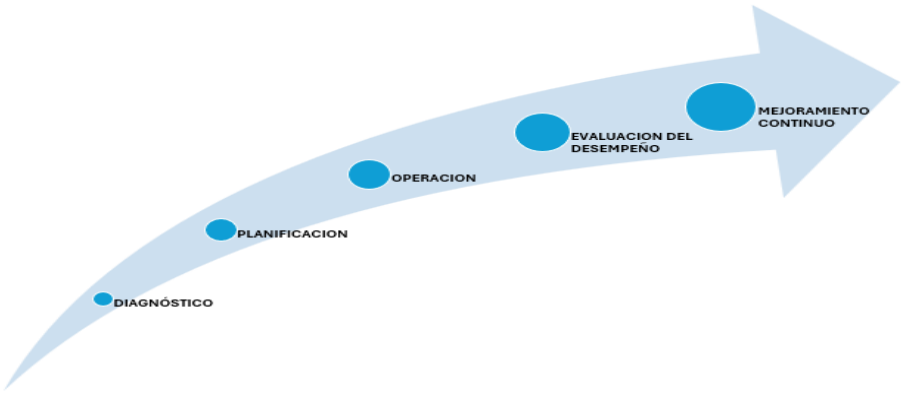
a) Contextualización al Informe De Seguimiento Al Modelo De Seguridad Y Privacidad De La Información (MSPI) en la ANCP – CCE.

En cumplimiento de las funciones asignadas al Área de Control Interno y en concordancia con los lineamientos del Modelo Estándar de Control Interno – MECI, se desarrolla el presente Informe de Seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI), con el propósito de verificar el adecuado avance, implementación y sostenibilidad de las acciones orientadas a garantizar la protección de la información institucional y el fortalecimiento de la gestión de la seguridad digital en la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE).

El MSPI constituye una herramienta fundamental para la administración pública, dado que orienta a las entidades en la gestión integral de los riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos de información, promoviendo una cultura de seguridad y privacidad conforme a las disposiciones de la Política de Gobierno Digital y a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Este modelo se estructura en cinco (5) fases interdependientes que permiten establecer un ciclo de mejora continua en materia de seguridad y privacidad de la información:

FASES Modelo de Seguridad y Privacidad de la Información (MSPI)



Elaboración: Propia de Control Interno

INFORME DE LEY – CONTROL INTERNO

1. **Diagnóstico:** Identificación del estado actual de la entidad frente a los requisitos del MSPI mediante un análisis (GAP), que sirve como base para la planificación y para medir los avances en etapas posteriores.

2. **Planificación:** Definición de necesidades, objetivos y estrategias en seguridad y privacidad de la información, considerando el mapa de procesos, el tamaño institucional y los contextos interno y externo, así como la valoración y tratamiento de riesgos.

3. **Operación:** Implementación de los controles y medidas definidas en la planificación, orientadas a mitigar los riesgos identificados y fortalecer las capacidades institucionales.

4. **Evaluación del desempeño:** Medición de la efectividad del modelo a través de auditorías, revisiones y análisis de indicadores, permitiendo identificar avances, desviaciones o áreas de mejora.

5. **Mejoramiento continuo:** Incorporación de acciones correctivas y preventivas que garanticen la evolución progresiva del sistema, fomentando la resiliencia institucional frente a los desafíos en materia de seguridad y privacidad de la información.

El seguimiento al MSPI permite a la entidad cumplir con su deber de vigilancia y control interno sobre los procesos relacionados con la gestión de la información, asegurando que las medidas adoptadas sean pertinentes, eficaces y estén alineadas con los principios de transparencia, eficiencia y protección de datos personales. De esta forma, el presente informe contribuye al fortalecimiento del Sistema de Control Interno y a la consolidación de un entorno digital seguro que respalde el cumplimiento de la misión institucional de la ANCP-CCE.

b) Resultados del Seguimiento.

Este informe se desarrolla bajo el principio de buena fe, con base en la información suministrada por parte de la Subdirección de Información y Desarrollo Tecnológico (IDT) de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE), consolidando las evidencias obtenidas en las diferentes etapas de verificación.

La Agencia Nacional de Contratación Pública – Colombia Compra Eficiente (ANCP-CCE), en cumplimiento de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), ha venido implementando desde el año 2024 el Modelo de Seguridad y Privacidad de la Información (MSPI) como parte integral de su Sistema de Gestión de Seguridad de la Información (SGSI). Esta implementación se ha consolidado como una estrategia transversal que busca garantizar la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información.

El informe presentado por la Subdirección de Información y Desarrollo Tecnológico (IDT) evidencia un avance en la adopción de políticas, procedimientos y controles técnicos y administrativos que fortalecen la seguridad digital de la entidad.

INFORME DE LEY – CONTROL INTERNO

La Subdirección de Información y Desarrollo Tecnológico a través de la información suministrada, mediante el informe de diciembre 2024, dentro de este ejercicio auditor – seguimiento dio a conocer que viene adelantando la implementación del MSPI en cumplimiento de las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), alineando sus acciones con la Política de Gobierno Digital y las normas ISO/IEC 27001 y 27002. Igualmente agrega que este modelo, aplicado desde el año 2024 hasta 2026, busca garantizar la protección integral de los activos de información y la madurez de los procesos asociados al Sistema de Gestión de Seguridad de la Información (SGSI). Durante el periodo de evaluación, se observa que la entidad ha logrado consolidar una estructura de gobierno de la seguridad de la información, sustentada en la definición de roles, responsabilidades, políticas específicas y mecanismos de seguimiento.

Si bien, la implementación del ciclo PHVA (Planear, Hacer, Verificar y Actuar) permite una gestión más eficiente de los riesgos tecnológicos, garantizando la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información, a través de este seguimiento se encontró:

- La actualización de la Política de Seguridad y Privacidad de la Información.
- La adopción de las guías del MSPI (gestión de riesgos, controles de seguridad, continuidad del negocio, seguridad en la nube y mejora continua).
- El fortalecimiento de los mecanismos de monitoreo y respuesta ante incidentes de seguridad de la información.

De lo cual se puede colegir que estas acciones avanzan a fin de lograr favorecer el aseguramiento de la información y la consolidación del Sistema de Gestión de Seguridad de la Información (SGSI) en la ANCP-CCE.

Para este ejercicio de seguimiento la Subdirección de Información y Desarrollo Tecnológico (IDT), los soportes aportados, no presentan suficiencia y consistencia que demuestren de manera verificable la existencia y ejecución de los controles establecidos en la actualidad. Asimismo, aunque en los comités de (COASIC) se reportan avances en el cumplimiento del MSPI, no se observaron evidencias documentales que respalden los resultados mencionados, sobre los cuales Control Interno y la misma entidad pueda tener la certeza de su existencia.

En este sentido, Control Interno considera necesario fortalecer la trazabilidad y documentación de los avances del MSPI, asegurando que cada actividad o control implementado cuente con la evidencia correspondiente que permita demostrar su efectividad y sostenibilidad. De igual forma, se recomienda que las evidencias derivadas de los comités técnicos y de seguridad sean registradas y consolidadas en el SharePoint que facilite el seguimiento continuo, la verificación de resultados y la evaluación de madurez frente a los lineamientos del MinTIC y las normas ISO aplicables.

Finalmente, se recomienda que la Subdirección de Información y Desarrollo Tecnológico articule sus informes de gestión con los criterios definidos en el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información

(MSPI), con el fin de fortalecer la transparencia en los procesos de reporte, la mejora continua y la rendición de cuentas sobre el estado de la seguridad de la información en la entidad.

En atención a lo anterior, se solicita la elaboración inmediata de un Plan de Mejoramiento, en el cual se registren y documenten las acciones correctivas y preventivas implementadas con plazos claros y razonados para cumplirlos. Dicho plan deberá incluir las evidencias y soportes correspondientes que permitan verificar la ejecución, eficacia y trazabilidad de cada actividad realizada, en cumplimiento con los lineamientos del Sistema de Control Interno.

RECOMENDACIONES DE CONTROL INTERNO

Considerando la información recopilada y los resultados del seguimiento, el equipo de Control Interno recomienda las siguientes acciones estratégicas para consolidar la implementación del MSPI y mejorar la madurez institucional en seguridad de la información, las cuales se presentan a continuación:

- Se recomienda establecer un Centro de Operaciones de Seguridad (SOC) institucional que permita el monitoreo continuo de los eventos de seguridad, la detección temprana de anomalías y la respuesta oportuna ante incidentes tecnológicos, fortaleciendo la capacidad de vigilancia, reacción y mitigación frente a amenazas que puedan comprometer la información institucional, cabe anotar que esta implementación esta en mora de aplicarse toda vez que deviene la necesidad de años atrás.

- De igual forma, conformar un Grupo de Respuesta a Incidentes de Seguridad de la Información (CSIRT interno) con personal especializado y roles definidos, encargado de coordinar las acciones técnicas y administrativas necesarias para contener, analizar y gestionar incidentes, garantizando la continuidad operativa y la resiliencia tecnológica de la entidad, es decir es un grupo operativo que bien puede integrarse de acuerdo a los perfiles que tiene la entidad.

- Implementar un tablero de control de cumplimiento del MSPI con indicadores de madurez, efectividad de controles y niveles de riesgo, que permita disponer de información precisa y oportuna para la toma de decisiones estratégicas y la mejora continua del sistema de gestión y que sea accesible para el monitoreo y control para la segunda línea de defensa.

- Actualizar de manera periódica el inventario de activos de información mediante validaciones cruzadas entre áreas responsables, con el fin de mantener un registro actualizado que refleje la realidad operativa y priorice la protección de los activos críticos conforme a los lineamientos del MSPI.

INFORME DE LEY – CONTROL INTERNO

- Fortalecer la seguridad de los servicios tecnológicos en la nube, asegurando el cumplimiento de los estándares internacionales ISO/IEC 27017 y 27018, lo cual contribuirá a la protección de los datos alojados y al incremento de la confianza institucional en el entorno digital, en búsqueda de implementar controles tangibles documentados, que den la certeza de evitar la duplicidad de la información e igual forma la información borrador "basura" que pudiera estar siendo alojada en la nube, lo cual no contribuye a la optimización del servicio de nube.

- Consolidar un programa integral de capacitación y sensibilización en ciberseguridad y protección de datos personales, que incluya simulaciones prácticas de incidentes y ejercicios de phishing, con el propósito de fortalecer la cultura de seguridad y reducir los riesgos asociados al factor humano.

- Establecer y mantener un procedimiento documentado para la gestión y trazabilidad de incidentes de seguridad, de manera que se fortalezcan las capacidades institucionales de respuesta, se minimicen los impactos y se garantice la continuidad del negocio.

- Realizar pruebas anuales de continuidad operativa y recuperación de información, asegurando que los mecanismos de respaldo y restauración sean efectivos ante contingencias tecnológicas o ciberataques.

- Formular política de seguridad física de la información.

- Finalmente, promover mecanismos de retroalimentación entre los usuarios y el área de seguridad de la información, que permitan identificar oportunidades de mejora, optimizar los controles implementados y fortalecer la confianza del personal en las medidas de protección institucional.

EDITH CARDENAS HERRERA

Firmado digitalmente por EDITH CARDENAS HERRERA
Fecha: 2025.11.10 17:30:05 -05'00'

Asesor(a) Experto(a) con Funciones de Control Interno

Aprobó	Edith Cárdenas Herrera
Revisó	Edith Cárdenas Herrera
Elaboró	Vidal de Jesús Garavito Castro
Fecha	10 de noviembre 2025
Código de Informe	52 - 1

INFORME DE LEY – CONTROL INTERNO

CONTROL DE CAMBIOS DEL DOCUEMNTO					
VERSION	**AJUSTES**	**FECHA**	**VERSIÓN ACTUAL**		**01**
01	Creación y estandarización de formato	01/07/2021	**Elaboró**	Judith Gómez	Asesora Experta con funciones de Control Interno
			Revisó	Judith Gómez	Asesora Experta con funciones de Control Interno
			Aprobó	Judith Gómez	Asesora Experta con funciones de Control Interno