TIPO DE INFORME:	Preliminar		Final	x

Tabla de contenido

Índice de tablas

1. **TÍTULO DE LA AUDITORÍA**
   Auditoría al Modelo de Privacidad y Seguridad de la Información (MSPI) / Norma ISO 27001: Seguridad de la Información.

2. **FECHA DE LA AUDITORÍA**
   Del 15 de agosto al 10 de diciembre de 2025.

3. **PERIODO EVALUADO**
   Abarca las actividades ejecutadas para la implementación y sostenibilidad del Modelo de Seguridad y privacidad de la información (MSPI) en Capital para el periodo comprendido entre el 1 de octubre de 2024 al 31 de julio de 2025.

4. **UNIDAD AUDITADA**
   Proceso de Gestión TIC

5. **LÍDER DE LA UNIDAD AUDITADA**
   Claudia Patricia Ardila Díaz – Subdirección Administrativa

6. **AUDITORES**
   Diana del Pilar Romero – Jizeth Hael González Ramírez

7. **OBJETIVO DE LA AUDITORÍA**
   Verificar el cumplimiento de la implementación del Modelo de Privacidad y Seguridad de la Información en Capital a través de la verificación de controles establecidos en la norma ISO: 27001:2013/2022.

8. **ALCANCE DE LA AUDITORÍA**
   Abarca las actividades ejecutadas para la implementación y sostenibilidad del Modelo de Seguridad y privacidad de la información (MSPI) en Capital para el periodo comprendido entre el 1 de octubre de 2024 al 31 de julio de 2025.

9. **LIMITACIÓN**
   Se identificó una limitación al alcance de la presente auditoría al no contar con la totalidad de información para evaluación, específicamente al no contar con los permisos de visualización de la herramienta estadística de gestión de incidentes relacionada como soporte de control en la matriz de *“Controles organizacionales”*.

10. **CRITERIOS**
    - Constitución política de Colombia
    - 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"

- Resolución 02277 DEL 03 de junio del 2025 del MinTic, “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”
- Resolución 500 de 2021 del MinTic, "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".
- Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG - Versión 6 - 2024.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6
- NTC ISO 27001:2013/2022.
- Modelo de Seguridad y Privacidad de la Información (MSPI) - MINTIC
- Manual metodológico para la Administración del riesgo - Canal Capital.
- Política de administración de riesgos - Canal Capital.
- Procedimientos, manuales, políticas, guías y demás documentos del Sistema Integrado de Gestión de Capital relacionados con el objetivo de la auditoría.
- Las demás normas pertinentes relacionadas con el objetivo de la auditoría.

11. METODOLOGÍA

De conformidad con la Guía de Auditoría Interna basada en riesgos para entidades públicas expedida por el Departamento Administrativo de la Función Pública – DAFP (versión 4, 2020), se emplearon los procesos de Planificación, Ejecución, Informe de Auditoría y Seguimiento del progreso de la auditoría interna basada en riesgos, de la siguiente manera:

Planificación

- Conocimiento de la unidad auditada y elaboración del Plan de Auditoría Individual.
- Definición del objetivo, alcance y tiempos de ejecución (cronograma).
- Preparación de papeles de trabajo de la revisión documental y procedimental respecto a los lineamientos del Modelo de Seguridad y privacidad de la Información.

Ejecución

- Comunicación de inicio de evaluación mediante Memorando 878 del 27 de agosto de 2025.
- De conformidad con el autodiagnóstico diligenciado por el proceso, para el periodo de enero a junio de 2025, se tomó una muestra aleatoria de 20 controles calificados con un nivel de cumplimiento del 100%
- Solicitud de información mediante Memorando 867 del 25 de agosto de 2025.
- Solicitudes de información adicional al área de TIC y Servicios Administrativos vía correos electrónico del 21 de octubre de 2025.
- Pruebas en campo el 20 y 21 de octubre de 2025 en las sedes de Quinta Camacho y la Calle 26.

- Modificación al programa de trabajo de la auditoría, comunicado mediante Memorando 1088 del 22 de octubre de 2025.

Informe de Auditoría

- Análisis de la información remitida (soportes) por la unidad auditable y demás áreas requeridas, así como análisis de las pruebas realizadas, con el fin de validar el cumplimiento de las disposiciones legales vigentes y demás normas aplicables con relación al modelo de relacionamiento integral con la ciudadanía.
- Consolidación y entrega del informe preliminar de auditoría a los líderes y/o responsables de la unidad auditable.
- Análisis de las respuestas remitidas en respuesta al informe preliminar de auditoría (Memorando 1338 de 2025) y elaboración del informe final de auditoría.

Seguimiento del progreso

- Solicitud de la formulación del Plan de Mejoramiento en la herramienta vigente respecto a las actividades que eliminen las causas de las observaciones encontradas a la entrega del informe final.
- Acompañamiento de la formulación del Plan de Mejoramiento al área.
- Análisis de la evaluación de la auditoría CCSE-FT-018 y presentación (por parte del jefe de la oficina de Control interno) al Comité Institucional de Coordinación de Control Interno para implementación de mejoras en el ejercicio de auditoría a la entrega del informe final.

12. SITUACIONES GENERALES

11.1. ASPECTOS POSITIVOS

- Se adelantó el diligenciamiento de la herramienta de “Controles Organizacionales” en los cuales se registra el avance de los diferentes controles identificados de tipo organizacional, físico, humano y tecnológico en el marco de la implementación del modelo de la seguridad y privacidad de la información de Canal Capital.

- Se evidenciaron acciones coordinadas entre el área de Tecnologías de la información y las comunicaciones – TIC, servicios administrativos, Dirección Operativa, Gestión Documental y el área Técnica con el fin de robustecer políticas de seguridad y privacidad de la información existentes en la entidad.

- Se cuenta con acciones de pruebas en materia de seguridad con ejercicios controlados que permiten la toma de decisiones respecto al tratamiento de incidentes, establecimiento de actividades documentadas de análisis de

tráfico y uso de los recursos en materia de tecnologías de la información al interior de la entidad.

- Formulación de proyectos que permiten robustecer la infraestructura de la entidad, y por ende, mejorar la seguridad de la información generada en la entidad, mediante la trazabilidad de hojas de ruta de cableado estructurado y el Plan Estratégico de Tecnologías de la Información y las Comunicaciones que le permiten al área identificar necesidades y posterior toma de decisiones institucionales.

11.2. ANÁLISIS DE LA IMPLEMENTACIÓN DEL MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN EN CAPITAL

Considerando la actualización del Modelo de Seguridad y Privacidad de la Información – MSPI, adoptado mediante la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, *"por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia*", el presente informe evaluó los lineamientos vigentes del modelo.

Para la evaluación realizada, la Oficina de Control Interno tomó como insumo el autodiagnóstico realizado por el área de Gestión TIC para el periodo de enero a junio de 2025, elaborado con base en la versión actualizada del MSPI. Atendiendo a la fase de transición hacia el nuevo marco y a las limitaciones reconocidas por el propio proceso, se procedió a seleccionar una muestra aleatoria conformada exclusivamente por controles calificados con el 100 % de cumplimiento en dicho autodiagnóstico. En consecuencia, no se incluyeron en la evaluación los controles reportados como "en proceso" o "sin implementar", teniendo en cuenta que el área TIC ha identificado esta situación como una debilidad del sistema que será abordada en las próximas vigencias, con el propósito de cerrar las brechas existentes y fortalecer progresivamente la implementación del MSPI.

Como resultado del autodiagnóstico realizado por el área Tic, se obtiene que la implementación de controles en Capital actualmente está en el siguiente estado:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	84	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	90	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	90	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	44	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		77	100	GESTIONADO

Ilustración 1 Evaluación de efectividad de controles enero a junio de 2025 - ISO 27001:2022 anexo A

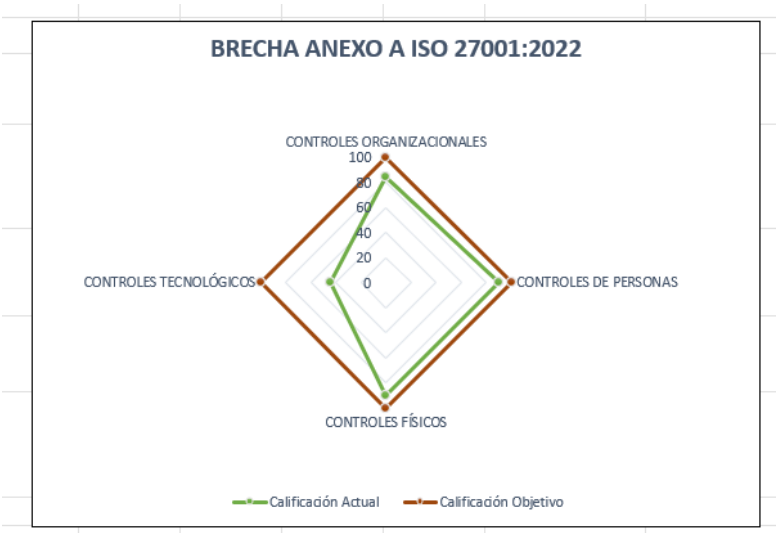


Ilustración 2 Brecha en la implementación de Controles

A continuación, se muestran los resultados de la evaluación adelantada a una muestra aleatoria de 20 controles calificados con 100 de cumplimiento:

Tabla 1 Verificación de controles calificados con un cumplimiento del 100%

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
A 5.3 / Segregación de funciones La organización debe determinar qué deberes y áreas de responsabilidad deben segregarse. Los siguientes son ejemplos de actividades que pueden requerir segregación: a) iniciar, aprobar y ejecutar un cambio; b) solicitar, aprobar e implementar derechos de acceso; c) diseñar, implementar y revisar el código; d) desarrollar software y administrar sistemas de producción; e) usar y administrar aplicaciones; f) utilizar aplicaciones y administrar bases de datos; g) diseñar, auditar y asegurar los controles de seguridad de la información.	No se reportó en el autodiagnóstico cómo Capital da cumplimiento a la implementación del control	Se evidencia que se creó el documento de roles y responsabilidades : Área de Gestión TIC, donde se e describen los roles estratégicos, tácticos y operativos del área TIC, así como las responsabilidades del Oficial de Seguridad de la Información y del Oficial de Protección de Datos. Si bien el documento evidencia una definición y segregación de funciones, este **no se encuentra formalizado dentro del Sistema Integrado de Gestión de Canal Capital**, lo que representa una debilidad en la trazabilidad y control documental. Se recomienda formalizar el documento en el Sistema de Gestión, con su respectiva codificación, aprobación y control de versiones, garantizando su consulta y actualización institucional. Adicionalmente, en el autodiagnóstico no se diligenció cómo Capital da cumplimiento al requisito normativo, por lo que se evidencia debilidades en el reporte integral de la herramienta de autoevaluación. **Respuesta al informe preliminar de auditoría:** El control se implementó mediante un documento de Roles y Responsabilidades interno y en uso, asegurando la segregación durante el periodo 10/2024 - 07/2025. La falta de formalización en el SIG es una mejora de la trazabilidad que está siendo considerada en el avance de la transición normativa, pero no es un incumplimiento del control base. **Análisis Oficina de Control Interno:** La objeción no desvirtúa la observación por lo tanto, esta **se mantiene.**		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		El control establece que la organización debe determinar y asegurar la segregación de funciones críticas (iniciar, aprobar, ejecutar; desarrollo, administración, auditoría, etc.). Para efectos de auditoría y aseguramiento: La segregación debe estar formalmente definida, aprobada y controlada. Debe ser verificable y trazable para terceros (auditoría interna/externa). Un documento interno no formalizado dentro del SIG no garantiza estos atributos. Que el documento esté "en uso" demuestra una práctica operativa; sin embargo: • No se evidenció aprobación formal por la instancia competente. • Codificación, control de versiones y vigencia. • Mecanismo de actualización y socialización institucional. En ausencia de estos elementos, la segregación **depende de prácticas internas** y no de un control organizacional plenamente establecido.		
A 5.7 / Inteligencia de amenazas Proporcionar conciencia del entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas. La inteligencia de amenazas debe ser: a) relevante (es decir, relacionado con la protección de la organización); b) perspicaz (es decir, proporcionar a la organización una comprensión precisa y detallada de la panorama de amenazas); c) contextual, para brindar conciencia situacional (es decir, agregar contexto a la información en función del	Se proyectó el plan de sensibilización del MSPI https://intranet.canalcapital.gov.co/intranet/docdowncc/DocSistema/2025/Plan/AGRI-SI-PL-005%20PLAN%20DE%20SENSIBILIZACION%20DEL%20SGSI.pdf	Para dar cumplimiento a este control, se deben cumplir los siguientes requisitos: 1. Que se proporcione conciencia del entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación adecuadas. 2. Que se implementen procesos para incluir información recopilada de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la organización. En el reporte del autodiagnóstico sólo se relaciona cómo se da cumplimiento al requisito 1 y verificados los soportes remitidos se evidencia que se han ejecutado las		x

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
momento de los eventos, dónde ocurren, experiencias previas y prevalencia en organizaciones similares); d) procesable (es decir, la organización puede actuar sobre la información de manera rápida y efectiva). Las actividades de inteligencia de amenazas deben incluir: a) establecer objetivos para la producción de inteligencia sobre amenazas; b) identificar, examinar y seleccionar fuentes de información internas y externas que sean necesarias y apropiadas para proporcionar la información requerida para la producción de inteligencia sobre amenazas; c) recopilar información de fuentes seleccionadas, que pueden ser internas y externas; d) procesar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o corroborando la información); e) analizar la información para comprender cómo se relaciona y es significativa para la organización; f) comunicarlo y compartirlo con personas relevantes en un formato que pueda ser entendido. La inteligencia de amenazas debe analizarse y utilizarse posteriormente: a) implementando procesos para incluir información recopilada de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la organización; b) como entrada adicional a controles técnicos preventivos y de detección como cortafuegos, detección de intrusos sistema o soluciones antimalware; c) como entrada a los procesos y técnicas de prueba de seguridad de la información. La organización debe compartir la inteligencia sobre amenazas con otras organizaciones de forma mutua para mejorar la inteligencia sobre amenazas en general.		actividades proyectadas en el plan de sensibilización con respecto a tips, charlas y ejercicios controlados de sensibilización y concientización que fortalecen la cultura de seguridad; sin embargo, en el memorando 1051 de 2025 el área de Sistemas indica que también se hace concienciación y comunicación en materia de seguridad y privacidad a través de "las cláusulas de confidencialidad y uso de la información están formalmente incluidas en los contratos firmados con proveedores", pero esta información no se reporta en el autodiagnóstico. Adicionalmente, no se reporta cómo se da cumplimiento a la gestión estructurada de inteligencia de amenazas, entendida como la recolección, análisis y uso sistemático de información sobre amenazas emergentes, vulnerabilidades o actores de riesgo, para lo cual recomienda establecer un documento formal para la inteligencia de amenazas, que contemple fuentes internas y externas (CERT, CSIRT, MinTIC, alertas del sector público), su análisis periódico y mecanismos de comunicación de alertas al personal TIC, lo anterior, teniendo en cuenta que no se evidencia este documento en el sistema de gestión de Capital. **Respuesta al informe preliminar de auditoría:** Se da cumplimiento al control con la concientización y la inclusión activa en la gestión de riesgos mediante las herramientas de monitoreo Fortigate, SOC, SIEM, Bitdefender y Reportes de Colcert. La recomendación de un "documento formal" para la gestión de inteligencia de amenazas va más allá del control base y es parte del robustecimiento que se adelanta en la transición al nuevo modelo (Resolución 02277)		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO

		Análisis Oficina de Control Interno:
		La objeción no desvirtúa la observación formulada, por lo que esta **se mantiene**, por las siguientes consideraciones:
		
		Contrario a lo señalado por el proceso, la recomendación de un documento formal no introduce un requisito adicional, sino que responde a la necesidad de evidenciar el cumplimiento de los literales del control A.5.7.
		
		• Un documento (o procedimiento formalizado) es el mecanismo mínimo para demostrar:
		
		  • Fuentes de inteligencia (por ejemplo, Colcert, CSIRT, MinTIC, proveedores).
		  • Periodicidad de análisis.
		  • Roles y responsabilidades.
		  • Mecanismos de comunicación y uso de la información.
		
		En ausencia de este instrumento, no se evidencia de forma trazable el cumplimiento integral del control.
		
		El informe preliminar reconoce el contexto de transición; sin embargo:
		• El proceso **autocalificó el control con un 100 % de cumplimiento**.
		• Al hacerlo, asume que **todos los requisitos del control están plenamente implementados**, no en fase de robustecimiento.
		• Si el control se encuentra en fortalecimiento, la calificación del 100 % **no resulta consistente** con el estado real de implementación.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
A 5.18 / Derechos de acceso Concesión y revocación de los derechos de acceso El proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico otorgados a la identidad autenticada de una entidad debe incluir: a) obtener autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados b) considerando los requisitos comerciales y la política y las reglas específicas del tema de la organización sobre control de acceso; c) considerar la segregación de funciones, incluida la segregación de las funciones de aprobación e implementación de los derechos de acceso y separación de roles en conflicto; d) garantizar que los derechos de acceso se eliminen cuando alguien no necesite acceder a la información y otros activos asociados, en particular garantizar que los derechos de acceso de los usuarios que han dejado la organización se eliminen de manera oportuna; e) considerar otorgar derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de vencimiento, en particular para el personal temporal o el acceso temporal requerido por el personal; f) verificar que el nivel de acceso otorgado esté de acuerdo con las políticas específicas del tema sobre control de acceso (ver 5.15) y sea consistente con otros requisitos de seguridad de la información, como la segregación de funciones (ver 5.3); g) garantizar que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de la autorización los procedimientos se completan con éxito;	Se asignan o revocan permisos de acceso físicos y lógicos, conforme a los términos de ejecución contractual, estos se controlan con la expedición de paz y salvos donde se deshabilitan usuarios de acceso a sistemas de información, correo, entre otros, y se solicita la devolución de las tarjetas de control de acceso	Durante las pruebas de auditoría se remitieron como soportes los siguientes documentos: • Guía de acceso y servicios de red (AGRI-SI-GU-008) • Manual de Políticas Complementarias de Seguridad de la Información (AGRI-SI-MN-006) • Manual de Gestión de Usuarios (AGRI-SI-MN-005) • Circular 6 de 2025 – Medidas de seguridad física • Guía de seguridad física y del entorno (AGRI-SI-GU-002) • Matriz con los usuarios con privilegios avanzados La evidencia demuestra la existencia de procedimientos documentados para otorgar y quitar derechos de acceso, así como un inventario de usuarios con privilegios controlados. **Recomendación:** Fortalecer el reporte en la herramienta de autodiagnóstico de todos los lineamientos que se tienen para este control.	x	

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
h) mantener un registro central de los derechos de acceso (…)				
A 5.19 / Responsable de seguridad de la Información: Seguridad de la información en las relaciones con proveedores 1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información y se han diseñado programas para los funcionarios de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están en 20. 2. Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección, están en 40. 3. Si se han ejecutado los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección, , están en 60.	Se cuenta con la Política de seguridad de la información formulado, aprobada e implementada, de igual manera en las minutas contractuales se les exige a los proveedores el cumplimiento de seguridad de la información. http://intranet.canalcapital.gov.co/intranet/docdowncc/DocSistema/2020/Pol%C3%ADtica/AGRI-SI-PO-002%20POL%C3%8DTICA%20DE%20SEGURIDAD%20Y%20PRIVACIDAD%20DE%20LA%20INFORMACI%C3%93N.pdf	Se evidencia que en la Política de Seguridad y Privacidad de la Información (AGRI-SI-PO-002, versión 05, 2020) publicada en la intranet institucional, se define responsabilidades y conductas aplicables a funcionarios, contratistas y terceros. El área TIC informa y de evidencia que en las minutas contractuales se exige a los proveedores el cumplimiento de las obligaciones de seguridad de la información conforme al SGSI. Sin embargo, el control hace referencia a que se debe verificar y reportar si: Si se observa en los funcionarios una conciencia de seguridad y privacidad de la información y se ejecutan planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información. Frente a lo anterior no hay ningún reporte en el autodiagnóstico que permita evidenciar cómo se ha dado cumplimiento para calificarlo en 100, por lo que se evidencian debilidades en el diligenciamiento de este. **Respuesta al informe preliminar de auditoría:** El control está implementado. La Política de Seguridad y Privacidad (AGRI-SI-PO-002) incluye responsabilidades para proveedores, y el cumplimiento de seguridad se exige en las minutas contractuales. El área reconoce la debilidad en el diligenciamiento integral del autodiagnóstico, pero no se encuentra un incumplimiento en la ejecución efectiva del control durante el periodo auditado **Análisis Oficina de Control Interno:** Dado que la objeción no desvirtúa la observación, esta **se mantiene:**		x

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		El control exige más que cláusulas contractuales generales, es decir, que requiere evidenciar: • Conciencia efectiva en seguridad de la información en funcionarios y terceros. • Ejecución documentada de planes de concientización, comunicación y divulgación en materia de seguridad. • Evidencia de que dichos planes han sido ejecutados, evaluados y ajustados, no solo formulados. No se evidenció en el autodiagnóstico ni se remiten soportes adicionales que permitan verificar: • Cómo se midió la conciencia de seguridad en proveedores. • Qué actividades específicas se ejecutaron para verificar el cumplimiento de las obligaciones de seguridad por parte de terceros. • Resultados, seguimiento o evaluación de dichas acciones		
A 5.26 / Responsable de seguridad de la información: Aprendizaje sobre los incidentes de seguridad de la información La organización debe establecer y comunicar procedimientos sobre la respuesta a incidentes de seguridad de la información a todas las partes interesadas relevantes. Los incidentes de seguridad de la información deben ser respondidos por un equipo designado con la competencia requerida (ver 5.24). La respuesta debe incluir lo siguiente: a) contener, si las consecuencias del incidente pueden	Se cuenta con la guía y formato de gestión de incidentes de seguridad de la información	En las pruebas adelantadas se evidencia que se cuenta con los siguientes reportes y documentos: 1. Bitácora de incidentes (octubre 2024 – julio 2025) con campos de fecha, tipo de incidente, responsable, acciones ejecutadas y estado. 2. Evidencias de lecciones aprendidas (pérdida de información y phishing: comunicación de alerta, denuncia ante Fiscalía, aplicación de DMARC/DKIM). 3. Ejercicio de phishing controlado realizado el 27 de junio de 2025. 4. Guía AGRI-SI-GU-007 “Gestión de Incidentes de Seguridad de la Información”, versión 04, formalizada	**x**	

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
extenderse, los sistemas afectados por el incidente; b) recolectar evidencia (ver 5.28) tan pronto como sea posible después de la ocurrencia; c) escalada, según sea necesario, incluidas las actividades de gestión de crisis y posiblemente invocando negocios planes de continuidad (ver 5.29 y 5.30); d) garantizar que todas las actividades de respuesta involucradas se registren correctamente para su posterior análisis; e) comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo a todas las partes interesadas internas y externas relevantes siguiendo el principio de necesidad de saber; f) coordinarse con partes internas y externas como autoridades, grupos y foros de interés externos, proveedores y clientes para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones; g) una vez solucionado satisfactoriamente el incidente, cerrarlo formalmente y registrarlo; h) realizar análisis forenses de seguridad de la información, según se requiera (ver 5.28); i) realizar un análisis posterior al incidente para identificar la causa raíz. (…)		y publicada en la intranet institucional. Se evidencia que la entidad cuenta con un procedimiento formal y vigente para la gestión de incidentes, el cual establece el ciclo completo de detección, análisis, contención, erradicación, recuperación y generación de lecciones aprendidas, alineado con el MSPI y la ISO/IEC 27001:2022. Además, se evidencia la aplicación práctica del procedimiento mediante la bitácora y las acciones preventivas derivadas de eventos reales. **Recomendación:** Fortalecer la trazabilidad de los incidentes registrados y las acciones de mejora implementadas, incluyendo análisis de tendencias y validación de eficacia de las medidas adoptadas, ya que esto último no se ve reflejado en la matriz de seguimiento. Asimismo, se sugiere actualizar el autodiagnóstico del MSPI para reflejar la existencia y aplicación del documento AGRI-SI-GU-007 y la evidencia práctica de su implementación.		
A 5.32/ Responsable de seguridad de la Información: Derechos de propiedad intelectual Se deben considerar las siguientes pautas para proteger cualquier material que pueda considerarse propiedad intelectual: a) definir y comunicar una política específica sobre la protección de los derechos de propiedad intelectual; b) publicar procedimientos para el cumplimiento de los derechos de propiedad intelectual que definan el uso	Se encuentra en el proceso interno de Gestión TIC.	El área de Sistemas indica a través del memorando 1051 de 2025 que no existe un documento institucional formalizado como Política de Propiedad Intelectual. Se menciona que los aspectos relacionados con la titularidad de derechos, confidencialidad, y uso de software y datos de terceros se gestionan a través de cláusulas contractuales y Acuerdos de Confidencialidad (NDA), los cuales regulan propiedad, uso y restricciones sobre activos de información y productos desarrollados.		x

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
conforme de software y productos de información; c) adquirir software solo a través de fuentes conocidas y acreditadas, para garantizar que los derechos de autor no sean infringido; d) mantener registros de activos apropiados e identificar todos los activos con requisitos para proteger derechos de propiedad intelectual; e) mantener prueba y evidencia de propiedad de licencias, manuales, etc.; f) garantizar que cualquier número máximo de usuarios o recursos [por ejemplo, unidades centrales de procesamiento (CPU)] permitido dentro de la licencia no se exceda; g) llevar a cabo revisiones para garantizar que solo se instalen software autorizado y productos con licencia; h) proporcionar procedimientos para mantener las condiciones apropiadas de la licencia; i) proporcionar procedimientos para desechar o transferir software a otros; j) cumplir con los términos y condiciones del software y la información obtenida de las redes públicas y fuentes externas; k) no duplicar, convertir a otro formato o extraer de grabaciones comerciales (video, audio) que no sea permitido por la ley de derechos de autor o las licencias aplicables; l) no copiar, total o parcialmente, normas (…)		Si bien la gestión contractual y los acuerdos de confidencialidad mitigan parcialmente los riesgos asociados a la propiedad intelectual, la entidad no cuenta con una política institucional formalizada que consolide los lineamientos aplicables a software, bases de datos, documentos y contenidos generados o adquiridos, tal como lo exige el control A.5.32 de la ISO/IEC 27001:2022. Se recomienda formular y adoptar una Política de Propiedad Intelectual institucional, aprobada por la Alta Dirección e integrada al Sistema de Gestión de Seguridad de la Información (SGSI), que defina de manera explícita: • Los criterios de titularidad, licenciamiento y uso de software y datos. • Las directrices para el tratamiento de derechos de autor, licencias open source y contenidos multimedia. • Los mecanismos de verificación de cumplimiento y actualización. Adicionalmente, se debe ajustar el autodiagnóstico del MSPI para reflejar esta brecha y el plan de acción correspondiente para su desarrollo e implementación. **Respuesta al informe preliminar de auditoría:** La gestión y protección de la Propiedad Intelectual se realiza mediante cláusulas contractuales específicas y Acuerdos de Confidencialidad (NDA). Esto asegura la protección de los activos durante el periodo auditado. La formalización de una política específica es una recomendación de mejora para la transición a la nueva normativa, pero el control en su contexto contractual está mitigado y operativo.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		La gestión y protección de la Propiedad Intelectual se realiza mediante cláusulas contractuales específicas y Acuerdos de Confidencialidad (NDA). Esto asegura la protección de los activos durante el periodo auditado. La formalización de una política específica es una recomendación de mejora para la transición a la nueva normativa, pero el control en su contexto contractual está mitigado y operativo. **Análisis Oficina de Control Interno:** La objeción no desvirtúa la observación por lo que esta **se mantiene**: El control exige una política y procedimientos institucionales, estableciendo de manera expresa que la organización debe: • Definir y comunicar una política específica sobre la protección de los derechos de propiedad intelectual. • Publicar procedimientos para el uso conforme de software y productos de información. • Mantener registros de licencias, evidencias de propiedad y revisiones periódicas. Las cláusulas contractuales y los NDA no sustituyen la exigencia de una política institucional formalizada, aprobada y comunicada. Y, dado que el proceso reconoce que la política está pendiente de formalización; en consecuencia: • El control **no se encuentra completamente implementado**.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		• La calificación del 100 % en el autodiagnóstico **no resulta consistente** con el estado real del control. • El argumento de transición refuerza la necesidad de ajustar la calificación y definir acciones.		
A 5.34 / Responsable de seguridad de la Información: Privacidad y protección de la PII La organización debe establecer y comunicar una política de privacidad y protección de PII específica del tema a todas las partes interesadas relevantes. La organización debe desarrollar e implementar procedimientos para la preservación de la privacidad y la protección de la información de identificación personal (PII). Estos procedimientos deben comunicarse a todas las partes interesadas relevantes involucradas en el procesamiento de información de identificación personal. El cumplimiento de estos procedimientos y de toda la legislación y los reglamentos pertinentes relacionados con la preservación de la privacidad y la protección de la PII requiere roles, responsabilidades y controles apropiados. A menudo, esto se logra mejor mediante el nombramiento de una persona responsable, como un oficial de privacidad, que debe brindar orientación al personal, los proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que deben seguirse. La responsabilidad por el manejo de la PII debe abordarse teniendo en cuenta la legislación y los reglamentos pertinentes. Se deben implementar medidas técnicas y organizativas apropiadas para proteger la PII.	Se cuenta con la política de tratamiento de datos personales	Durante las pruebas de auditoría se remitieron como soportes los siguientes documentos: • Política de Seguridad y Privacidad de la Información (AGRI-SI-PO-002) actualizada y aprobada por el CIGD el 02/10/2025. • Respuesta del área TIC indicando que la política anterior estaba en actualización y que la nueva versión se encuentra en proceso de publicación y socialización. • Se referencia a la Política de Tratamiento de Datos Personales, como documento que regula el ciclo de vida de la PII (recolección, procesamiento, transmisión, almacenamiento, eliminación o Anonimización). • Se menciona que no se realizaron socializaciones durante el periodo auditado, por estar en trámite de aprobación, aunque se adjuntan soportes de planificación y actas de comité y que, adicionalmente, desde el área de sistemas se han realizado o se tiene programado para la vigencia 2025 realizar sensibilización y comunicación al personal sobre respeto a los derechos de autor puesto que "*el área de Gestión TIC no es el responsable de aplicar las normas o regulaciones en el marco de la propiedad intelectual (derechos de autor), sin embargo podemos apoyar a las áreas involucradas y cuyas funciones están en emitir y dirigir normas y reglamentaciones sobre su uso para alinearlas con las mejores prácticas del SGSI, en materia de confidencialidad, integridad y disponibilidad si así se requiere*" Frente a lo anterior, se evidencia que la entidad cuenta con una política formal y vigente que regula la privacidad y el tratamiento de la PII, alineada con la Ley 1581 de 2012, el	**x**	

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		Decreto 1377 de 2013 y la ISO/IEC 27001:2022. **Recomendación:** Fortalecer la articulación entre el área TIC y las dependencias responsables de la implementación del MSPI y de la protección de datos personales, asegurando coherencia entre los controles técnicos y los jurídicos. Finalmente, el autodiagnóstico debe actualizarse para reflejar el avance en la aprobación y socialización de la política, así como las responsabilidades compartidas entre TIC y Jurídica, y que el área Jurídica reporte los avances en el cumplimiento de este control y el área de Gestión del seguimiento a la ejecución del control actuando en este caso como segunda línea de defensa.		
A 5.37 / Responsable de seguridad de la Información: Procedimientos operativos documentados Se deben preparar procedimientos documentados para las actividades operativas de la organización asociadas con la seguridad de la información, por ejemplo: a) cuando la actividad deba ser realizada de la misma manera por muchas personas; b) cuando la actividad se realiza raramente y cuando se realiza la próxima vez es probable que el procedimiento tenga sido olvidado; c) cuando la actividad sea nueva y presente un riesgo si no se realiza correctamente; d) antes del traspaso de la actividad al nuevo personal. Los procedimientos operativos deben especificar: a) las personas responsables; b) la instalación y configuración segura de sistemas; c) procesamiento y manejo de información, tanto	Se cuenta con alguna documentación por parte de Gestión TIC	El reporte realizado por el área en el autodiagnóstico no es preciso, ni permite determinar cómo se da cumplimiento al requisito normativo., el reporte “Se cuenta con alguna documentación por parte de Gestión TIC" deber ser desarrollado y debe indicar explícitamente cómo se da cumplimiento al control. En las pruebas realizadas se evidencia que el área de Gestión TIC dispone de los siguientes documentos: • Procedimiento de copias de seguridad. • Manual de Políticas Complementarias. • Bitácora de respaldos. • Guía para el cifrado de la información. • Formato RFC (Request For Change). Se evidencia que estos documentos están publicados en la intranet y se remiten soportes de que fueron socializados en reuniones de seguimiento **con el equipo técnico.**		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
automatizado como manual; d) respaldo (ver 8.13) y resiliencia; e) requisitos de programación, incluidas las interdependencias con otros sistemas; f) instrucciones para el manejo de errores u otras condiciones excepcionales [por ejemplo, restricciones en el uso de programas de utilidad (ver 8.18)], que pueden surgir durante la ejecución del trabajo; g) contactos de soporte y escalamiento, incluidos contactos de soporte externo en caso de imprevistos dificultades operativas o técnicas; h) instrucciones de manejo de medios de almacenamiento (ver 7.10 y 7.14); i) procedimientos de reinicio y recuperación del sistema para su uso en caso de falla del sistema) la gestión de la pista de auditoría y la información de registro del sistema (ver 8.15 y 8.17) (…)		Sin embargo, las evidencias de socialización están dirigidas únicamente al equipo técnico de Gestión TIC, pero no se demuestra un proceso formal de formación, actualización o verificación de competencias, ni una periodicidad establecida para dichas socializaciones, teniendo en cuenta especialmente todos los controles establecidos en el Manual de Políticas Complementarias que establece controles no solo para el equipo Técnico de Gestión TIC sino para todos los colaboradores de Capital. Adicionalmente, al presentarse debilidades en otros controles de tipo organizacionales o tecnológicos, calificados con nivel de cumplimiento cero (0) y los cuáles requieren documentación por ejemplo el control A 8.1 dónde se debe documentar una política específica del tema sobre la configuración y el manejo seguros de los dispositivos de punto final del usuario, no se puede indicar que todas las actividades asociadas a seguridad de la información estén documentadas. Se recomienda actualizar el autodiagnóstico MSPI para reflejar de manera completa la documentación existente y las brechas pendientes. **Respuesta al informe preliminar de auditoría:** La documentación esencial está formalizada y los procedimientos clave fueron socializados al equipo técnico para asegurar la continuidad operativa y la ejecución efectiva de las tareas de seguridad (ej. Guía de Incidentes). La socialización con el resto de los colaboradores se realiza mediante la divulgación de piezas gráficas vía correo electrónico y boletines informativos en intranet. Se acoge la recomendación de periodicidad como una mejora del Plan de Transición.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		Análisis Oficina de Control Interno: La objeción no desvirtúa la observación, por lo que esta **se mantiene**: Sí se reporta que falta realizar capacitación, socialización o apropiación de los procedimientos, no es técnicamente procedente asignar una calificación del 100 % de cumplimiento, dado que el control exige no solo la existencia documental, sino su conocimiento, aplicación y uso efectivo por las partes interesadas relevantes. • De igual forma, se reitera que el enunciado utilizado en el autodiagnóstico consiste en que "se cuenta con alguna documentación" resulta impreciso y poco técnico, ya que: ➢ No permite identificar qué procedimientos específicos dan cumplimiento al control. ➢ No evidencia si la documentación cubre la totalidad de actividades operativas asociadas a la seguridad de la información. ➢ No permite verificar estado de aprobación, vigencia, alcance ni responsables, elementos mínimos para sustentar el cumplimiento integral del control.		
A 6.2 / Términos y condiciones de empleo Las obligaciones contractuales para el personal deben tener en cuenta la política de seguridad de la información de la organización y las políticas específicas del tema relevante. Además, se pueden	En los procesos de selección de personal se realiza a través de los procesos internos definidos por el área de recursos humanos, y para los procesos contractuales se realiza	Se incluye en las condiciones contractuales por parte de Canal Capital las cláusulas décimas quintas (Derechos de autor y conexos) y décima sexta (Confidencialidad y uso de la información); sin embargo, es importante que el área establezca de manera clara y precisa los soportes que dan	**x**	

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
aclarar y señalar los siguientes puntos: a) acuerdos de confidencialidad o no divulgación que el personal al que se le da acceso a información confidencial información debe firmar antes de tener acceso a la información y otros activos asociados (ver 6.6); b) responsabilidades y derechos legales [por ejemplo, con respecto a las leyes de derechos de autor o la legislación de protección de datos (ver5.32 y 5.34)]; c) responsabilidades para la clasificación de la información y la gestión de la organización información y otros activos asociados, instalaciones de procesamiento de información y servicios de información manipulado por el personal (ver 5.9 a 5.13); d) responsabilidades por el tratamiento de la información recibida de los interesados; e) acciones a tomar si el personal ignora los requisitos de seguridad de la organización (ver 6.4). (...)	a través del área de contratación de la entidad.	cumplimiento a los controles (teniendo en cuenta la transversalidad del modelo). Dentro de ello, se identifican mecanismos existentes adicionales como el formato de Compromiso ético del auditor interno (Anexo del Código de ética del auditor interno - Oficina de Control Interno), así como lineamientos desde la Política de tratamiento de datos personales y autorización de tratamiento de datos personales, al igual que la Política de seguridad y privacidad de la información, respecto al compromiso de los diferentes actores responsables de la información (la cual se recomienda actualizar de manera periódica, dado que la última actualización se adelantó en 2023), y, el formato "Compromiso de confidencialidad, reserva y no divulgación de la información".		
A 6.3 / Concientización, educación y entrenamiento en seguridad de la información Los acuerdos de confidencialidad o de no divulgación deben abordar el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. Con base en los requisitos de seguridad de la información de una organización, los términos de los acuerdos deben determinarse tomando en consideración el tipo de información que se manejará, su nivel de clasificación, su uso y el acceso permitido por la otra parte. Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se deben considerar los siguientes elementos: a) una definición de la información a proteger (por ejemplo, información confidencial);	Se tiene proyectado el plan sensibilización del SGSI	Se contempla un documento denominado "AGRI-SI-PL-005 PLAN DE SENSIBILIZACIÓN DEL SGSI (Cronograma)" el cual no contempla la vigencia en la cual se ejecutará, así como tampoco refiere el objetivo, ni herramienta de seguimiento a las actividades programadas. En consecuencia, de las ocho (8) actividades que se proyectan, se cuenta con soportes de dos (2) enmarcadas en ejercicios de phishing y uso responsable de la IA. Con base en lo mencionado, es importante que el área proyecte para las vigencias futuras un plan de concientización, educación y entrenamiento en materia de seguridad de la información que contemple: * Definición de información confidencial * Duración de los acuerdos de confidencialidad sobre la información, para lo cual deberá coordinarse con Gestión Documental, respecto a la inclusión del cuadro de		x

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
b) la duración esperada de un acuerdo, incluidos los casos en que puede ser necesario mantener confidencialidad por tiempo indefinido o hasta que la información esté disponible públicamente; c) las acciones requeridas cuando se termina un acuerdo; d) las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada; e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial; f) el uso permitido de la información confidencial y los derechos del firmante para usar la información; g) el derecho a auditar y monitorear actividades que involucren información confidencial para personas altamente sensibles circunstancias. (…)		clasificación documental e inventario de información clasificada y reservada, responsabilidades de la divulgación de información por parte de los diferentes actores, derechos de los firmantes, términos de la devolución y destrucción de la información (contemplados en las diferentes políticas institucionales, así como en las cláusulas de las condiciones contractuales), al igual que las acciones previstas a tomar en caso del incumplimiento de los diferentes acuerdos establecidos. Lo anterior, dando cumplimiento a la totalidad de condiciones establecidas en el control, adelantando seguimientos periódicos a las actividades, lo que permite reflejar el avance real de lo formulado. **Respuesta al informe preliminar de auditoría:** El plan de sensibilización existe (AGRI-SI-PL005) y se ejecutaron actividades clave (ej. Ejercicios de phishing, uso de IA), lo que demuestra la aplicación del control. La necesidad de más detalle y seguimiento para robustecer la cultura de seguridad es una mejora reconocida y está contemplada en el Plan de Mejoramiento que se presentó y socializó ante el CIGD. **Análisis Oficina de Control Interno:** Dado que la objeción no desvirtúa la observación, esta **se mantiene**: El control solicita un programa estructurado y continuo de concientización, educación y entrenamiento que incluya, entre otros: Objetivos claros y alcance institucional.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		Identificación de públicos objetivo. Contenidos diferenciados según roles. Periodicidad definida. Mecanismos de seguimiento y evaluación de eficacia. En el periodo evaluado: • El Plan AGRI-SI-PL-005 no define vigencia, objetivos, indicadores ni herramientas de seguimiento. • De las actividades proyectadas, no se evidenció la ejecución de la totalidad de las actividades propuestas. • No se cuenta con evidencia de evaluación de resultados ni retroalimentación. • La inclusión de acciones en el Plan de Mejoramiento no sustituye la evidencia requerida para sustentar la calificación del 100 % en el periodo evaluado.		
A 6.6 / Acuerdos de confidencialidad o no divulgación Los acuerdos de confidencialidad o de no divulgación deben abordar el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. Con base en los requisitos de seguridad de la información de una organización, los términos de los acuerdos deben determinarse tomando en consideración el tipo de información que se manejará, su nivel de clasificación, su uso y el acceso permitido	Se cuenta con el formato de compromiso de acuerdos de confidencialidad, reserva y no divulgación de la información	Se cuenta con el documento "AGTH-FT-083 COMPROMISO DE CONFIDENCIALIDAD, RESERVA Y NO DIVULGACIÓN DE LA INFORMACIÓN" del área de Recursos Humanos del 8 de abril de 2025, el cual contempla la definición de la información a proteger, duración del acuerdo, acciones al término de este, responsabilidades de los actores del acuerdo, uso de la información, términos y sanciones; sin embargo, no se mencionan aspectos clave como: e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial; f) el uso permitido de la información confidencial y los		x

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
por la otra parte. Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se deben considerar los siguientes elementos: a) una definición de la información a proteger (por ejemplo, información confidencial); b) la duración esperada de un acuerdo, incluidos los casos en que puede ser necesario mantener confidencialidad por tiempo indefinido o hasta que la información esté disponible públicamente; c) las acciones requeridas cuando se termina un acuerdo; d) las responsabilidades y acciones de los signatarios para evitar la divulgación de información no autorizada; e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial; f) el uso permitido de la información confidencial y los derechos del firmante para usar la información; g) el derecho a auditar y monitorear actividades que involucren información confidencial para personas altamente sensibles circunstancias; h) el proceso de notificación y reporte de divulgación no autorizada (…)		derechos del firmante para usar la información; g) el derecho a auditar y monitorear actividades que involucren información confidencial para personas altamente sensibles circunstancias; h) el proceso de notificación y reporte de divulgación no autorizada o información confidencial fuga. Por lo que se deberá verificar de manera coordinada entre el área de Tecnologías de la Información y las Comunicaciones y Talento Humano, con el fin de actualizar las políticas pendientes que den cabal cumplimiento a lo requerido por el control. **Respuesta al informe preliminar de auditoría:** El formato de Compromiso de Confidencialidad (AGTH-FT-083) existe y cubre la mayoría de los puntos. Los aspectos faltantes se gestionan en cláusulas contractuales específicas (PI,Auditoría) y la Guía de Incidentes. Se acoge la recomendación como una mejora necesaria para la armonización y unificación de documentos con Talento Humano en la fase de transición. **Análisis Oficina de Control Interno:** El control establece que los acuerdos de confidencialidad o no divulgación deben abordar explícitamente la totalidad de los elementos mínimos, entre ellos: • Definición de la información a proteger. • Duración del acuerdo. • Acciones al término del vínculo. • Responsabilidades y sanciones.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		• Propiedad de la información y derechos de propiedad intelectual. • Uso permitido de la información y derechos del firmante. • Derecho a auditar y monitorear. • Proceso de notificación y reporte de divulgación no autorizada. El propio proceso reconoce que el formato no cubre la totalidad de los requisitos, por lo tanto, un acuerdo que no contempla todos los literales del control no puede calificarse al 100 %.		
A 6.8 / Reporte de eventos de seguridad de la información Todo el personal y los usuarios deben ser conscientes de su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información. También deben conocer el procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se deben informar los eventos. El mecanismo de presentación de informes debe ser lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, violaciones y vulnerabilidades. Las situaciones a considerar para el reporte de eventos de seguridad de la información incluyen: a) controles de seguridad de la información ineficaces; b)incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información; c)errores humanos;	Se realizan los reportes a Gestión TIC y de acuerdo a su clasificación, se documentan en el formato de reporte de incidentes de seguridad y/o en informes	Si bien la entidad cuenta con un una Guía de gestión de incidentes de la seguridad de la información actualizado en agosto de 2025, el cual detalla las actividades de reporte y tratamiento, a la fecha no se han establecido jornadas de socialización respecto al documento que permita a los colaboradores de la entidad conocer el proceso de informe de eventos, el mecanismo y el resultado del reporte del incidente. De igual manera, se registra en una base de datos no identificada (contrario a lo relacionado en el soporte de ejecución del control) dos incidentes reportados en enero y mayo de 2025; sin embargo, no se cuenta con el registro de incidentes informados por la Oficina de Control Interno, correos que fueron remitidos al profesional de Seguridad de la Información en agosto de 2025, los cuales corresponden a una invitación de participación de carpetas contenidas en Google Drive, a pesar de que se marcó como spam por parte del área continuaban remitiéndose ese tipo de correos desde cuentas @gmail.com. Por lo que se recomienda: * Hacer uso del formato indicado en los soportes de ejecución del control.		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
d) incumplimiento de la política de seguridad de la información, políticas específicas del tema o normas aplicables; e) incumplimientos de las medidas de seguridad física; f) cambios del sistema que no han pasado por el proceso de gestión de cambios; g) mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware; h)infracciones de acceso; i)vulnerabilidades; j) sospecha de infección por malware.		* Hacer el registro de la totalidad de incidentes reportados con el fin de clasificarlos, disponer de la información mencionada en el numeral 8.3. de la Guía de gestión de incidentes de la seguridad de la información como hora del incidente, recursos afectados, impacto, fecha y hora de la solución del incidente. * Determinar la situación que conllevó a la ocurrencia del incidente, teniendo en cuenta los literales relacionados en la descripción del control. **Se recomienda** efectuar la socialización de los resultados de gestión efectuada a los reportantes, con el fin de que se guarde la trazabilidad de la totalidad del proceso adelantado por el área TIC. **Respuesta al informe preliminar de auditoría:** Se cuenta con la Guía de Gestión de Incidentes (AGRI-SI-GU-007) y una Bitácora de incidentes, demostrando la existencia y uso del procedimiento en el periodo auditado. La recomendación de socialización general y el uso riguroso del formato son mejoras de trazabilidad y cultura, no un incumplimiento del control. Se garantiza la gestión de la información sobre incidentes. **Análisis Oficina de Control Interno:** La objeción no desvirtúa la observación, por lo que esta **se mantiene**: El control establece que, todo el personal y los usuarios deben conocer: Su responsabilidad de reportar eventos. El procedimiento. El punto de contacto. El mecanismo de reporte debe ser fácil, accesible y disponible.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		Debe existir trazabilidad completa de los eventos reportados. Durante la auditoría se evidenció que: ➢ La bitácora **no contenía la totalidad de los eventos reportados** (incluidos correos maliciosos informados por la OCI). ➢ Se utilizaron **registros paralelos** y no el formato definido en la guía. ➢ No se cuenta con evidencia de: ➢ Clasificación completa de eventos. ➢ Registro de impactos, tiempos de atención y cierre. Esto indica una aplicación parcial de lo establecido en el control, por lo cual no puede calificarse con un cumplimento del 100 %.		
A 7.1 / Perímetros de seguridad física Las siguientes pautas deben considerarse e implementarse cuando corresponda para los perímetros de seguridad física: a) definir los perímetros de seguridad y la ubicación y resistencia de cada uno de los perímetros de acuerdo con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro) tener perímetros físicamente sólidos para un edificio o sitio que contenga procesamiento de información instalaciones (es decir, no debe haber espacios en el perímetro o áreas donde un robo pueda ocurrir fácilmente). Los techos exteriores, paredes, techos y pisos del sitio deben ser de construcción sólida y todos las puertas exteriores deben estar adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, rejas, alarmas, cerraduras). Las	Se cuenta con las respectivas medidas de seguridad, alarmas, controles de acceso biométricos y RFID, guardas de seguridad, entre otros.	Teniendo en cuenta la respuesta del área de Tecnologías de la Información se consultó con el área de Servicios Administrativos respecto a las pautas para implementar los perímetros de seguridad física, dentro de lo cual se indica que: *"Canal Capital realiza anualmente, a través de los contratos de vigilancia suscritos, el contratista realiza unos estudios de seguridad en los puntos donde se presta el servicio quien emite recomendaciones de mejora con el fin de fortalecer la seguridad de la Entidad. En ese sentido, remitimos los estudios de seguridad realizados en el año 2024 por el contratista actual. Asimismo, se aclara que para la vigencia en curso estos estudios se realizarán una vez finalice la convocatoria pública actualmente en desarrollo y se suscriba el nuevo contrato de vigilancia. En cuanto a las acciones de mejora producto de dichos estudios, en efecto, se evalúan desde la supervisión del contrato y posteriormente, se realizan cuando haya lugar con el fin de mejorar las condiciones de seguridad de las sedes del Canal".*		**x**

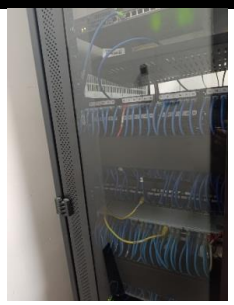
Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
puertas y ventanas deben cerrarse con llave cuando estén desatendidas y en el exterior. se debe considerar la protección de las ventanas, particularmente a nivel del suelo; puntos de ventilación también debe ser considerado; c) alarmar, monitorear y probar todas las puertas contra incendios en un perímetro de seguridad junto con el paredes para establecer el nivel de resistencia requerido de acuerdo con las normas adecuadas. Ellos deben operar a prueba de fallas.		Sin embargo, verificados los soportes remitidos por el área no se evidencian los resultados de la ejecución de pruebas sobre los perímetros definidos que contemplen alarmas, cerraduras, entre otros que impidan el ingreso. Dentro de los estudios efectuados por la empresa de seguridad contratada, se identifican puntos vulnerables y recomendaciones sobre las dos sedes, sin que se observen los soportes de la corrección de las vulnerabilidades. Por último, dentro de la ejecución del contrato no es posible evidenciar que se adelanten pruebas de los mecanismos y lineamientos en materia de seguridad, por lo que es importante que se articulen los esfuerzos y trabajos entre las áreas, efectuando solicitudes de pruebas, registro de resultados, implementación de acciones de mejora; lo que permitirá el fortalecimiento de la ejecución de controles requeridos a nivel institucional. **Respuesta al informe preliminar de auditoría:** La gestión documental y planificación están implementadas: se remitieron los estudios de seguridad del contratista que definen perímetros y debilidades. Las pruebas y correcciones son acciones de ejecución que están en curso, sujetas a procesos contractuales (nuevo contrato de vigilancia), y los documentos que fueron trasladados por competencia a Gestión de Recursos Administrativos. El control se considera implementado a nivel de gestión y planeación del MSPI. **Análisis Oficina de Control Interno:** La objeción no desvirtúa la observación, por lo que esta **se mantiene:**		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		El control establece que los perímetros de seguridad física deben: • Estar definidos, implementados, probados y mantenidos. • Contar con mecanismos efectivos de control de acceso, monitoreo y protección. • Ser objeto de pruebas periódicas y corrección de vulnerabilidades identificadas. Durante la auditoría se evidenció que: • Los estudios de seguridad identifican vulnerabilidades en las sedes. • No se evidencian soportes de ejecución de pruebas, corrección de hallazgos ni verificación de efectividad. • La ausencia de evidencias de cierre implica que los perímetros no estaban operando conforme al control durante el periodo evaluado. El traslado de documentos a Gestión de Recursos Administrativos: • Confirma la naturaleza transversal del control. • No sustituye la responsabilidad de articulación, seguimiento y reporte dentro del MSPI. • Refuerza la observación sobre desarticulación en el reporte del autodiagnóstico, pues solo lo diligenció el área de Gestión TIC sin el reporte de otras dependencias.		
A 7.6 / Trabajar en áreas seguras Las medidas de seguridad para trabajar en áreas seguras deben aplicarse a todo el personal y cubrir todas las actividades que se desarrollen en el área segura.	En el manual de políticas de seguridad de la información complementarias, se establecen directrices para la protección de áreas seguras. Así mismo, existen	Adelantada la consulta sobre el establecimiento de políticas para trabajo en zonas seguras, se informó por parte del área de Tecnologías de la Información y las Comunicaciones que no se cuenta con prohibiciones de equipos fotográficos y de vídeo, así como que no se puede limitar porque parte hace parte de las evidencias de los		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
Se deben considerar las siguientes pautas: a) informar al personal solo de la existencia de, o actividades dentro de, un área segura en caso de necesidad saber base; b) evitar el trabajo sin supervisión en áreas seguras tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas; c) cerrar físicamente e inspeccionar periódicamente las áreas seguras vacantes; d) no permitir que los equipos fotográficos, de video, de audio u otros equipos de grabación, como cámaras en el usuario dispositivos terminales, a menos que estén autorizados; e) controlar adecuadamente el transporte y uso de los dispositivos de punto final del usuario en áreas seguras; f) publicar los procedimientos de emergencia de manera fácilmente visible o accesible.	formatos y procedimientos para el control de acceso a áreas seguras.	informes mensuales de los colaboradores de la entidad, al ser soportes anexos. Sin embargo, se cuenta con acuerdos de confidencialidad con los contratistas (Cláusula de la minuta contractual). Teniendo en cuenta lo anterior, así como el Manual de políticas complementarias de seguridad de la información, no se observa que se cuente con lineamientos relacionados con las medidas de seguridad que se aplican en la entidad, teniendo en cuenta la identificación de parámetros físicos, así como tampoco se mencionan medidas de control de transporte, ni fue concertado con la Oficina de Control Interno las políticas de verificación integradas, así como tampoco se observan soportes de concertación de integración de políticas complementarias que se vienen efectuando por parte de áreas como Servicios Administrativos (salida y entrada de quipos) y el área Técnica. Dado lo indicado, se recomienda al área definir articuladamente las políticas operacionales del manual mencionado, que conserve la transversalidad de los procesos efectivamente ejecutados en el Canal. **Respuesta al informe preliminar de auditoría:** El Manual de Políticas Complementarias establece directrices. La restricción de equipos de grabación es difícil por la misionalidad de la entidad (audiovisual), y se mitiga con los Acuerdos de Confidencialidad. La recomendación de articulación y armonización de políticas se acoge como recomendación del Plan de Mejoramiento, dado el alcance de la auditoría.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		Análisis Oficina de Control Interno: Teniendo en cuenta lo indicado por el área **se mantiene** la observación.		
A 7.7 / Escritorio despejado y pantalla despejada La organización debe establecer y comunicar una política específica del tema sobre escritorio despejado y pantalla despejada a todas las partes interesadas relevantes. Se deben considerar las siguientes pautas: a) guardar bajo llave la información comercial confidencial o crítica (p. ej., en papel o en almacenamiento electrónico) multimedia) (idealmente en una caja fuerte, gabinete u otra forma de mueble de seguridad) cuando no se requiera, especialmente cuando el cargo quede vacante; cada dependencia tablas de retención b) proteger los dispositivos de punto final del usuario mediante cerraduras con llave u otros medios de seguridad cuando no estén en uso o desesperado) dejar los dispositivos de punto final de usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando están desatendidos. Todas las computadoras y sistemas deben configurarse con una función de tiempo de espera o cierre de sesión automático; reglas de bloqueo directorio activo y socialización d) hacer que el originador recopile los resultados de las impresoras o dispositivos multifunción de inmediato. El uso de impresoras con una función de autenticación, de modo que los creadores sean los únicos que puedan obtener sus impresiones y solo cuando estén parados al lado de la impresora; contrato con tercero de impresión uso de control de acceso e) almacenar de forma segura documentos y medios	Se cuenta con el manual de políticas complementarias, donde se estipulan los lineamientos	Si bien Canal Capital cuenta con el Manual de Políticas Complementarias de Seguridad de la Información actualizado el 10 de julio de 2025, en el cual se establecen 8.9.1 Normas generales para el mantenimiento del escritorio y pantalla limpia, así mismo, se cuenta con un espacio de gestión documental el cual se encuentra bajo llave, el centro de almacenamiento tanto de la Calle 69 y Calle 26 cuenta con puertas que cuentan con sistemas de seguridad para el acceso; sin embargo, a la fecha no se cuenta con recopilación de datos de los dispositivos multifunción, ni autenticación que permita ejercer control sobre las impresiones. De igual manera, se mencionan políticas de eliminación y/o borrado de información; no obstante a la fecha de evaluación no se cuenta con soportes que permitan evidenciar la ejecución de dichas actividades, al no conservar un registro de los equipos que son sometidos a borrado previo a la baja o reasignación. Así mismo, **se recomienda** que el área de conformidad con lo indicado en el documento adelante la socialización de los lineamientos indicados ya que se desconocen por parte de los colaboradores las Normas dirigidas a todos los Funcionarios, Proveedores, Socios de Negocio y Terceros; así mismo, **se recomienda**, complementar los procedimientos implementados al desocupar las instalaciones, incluida la realización de un barrido final antes de irse para garantizar que los activos de la organización no se queden atrás (por ejemplo, documentos caídos detrás de cajones o muebles) teniendo en cuenta que estos no son mencionados en el manual descrito.		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
de almacenamiento extraíbles que contengan información confidencial y, cuando ya no se necesiten, desecharlos mediante mecanismos seguros de eliminación (…)				
A 7.12 / Seguridad del cableado Se deben considerar las siguientes pautas para la seguridad del cableado: a) las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información sean subterráneas cuando sea posible, o estén sujetas a una protección alternativa adecuada, como protectores de cables en el piso y postes de servicios públicos; si los cables son subterráneos, protegerlos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia); b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen: 1) instalación de conductos blindados y cuartos o cajas cerradas y alarmas en los puntos de inspección y terminación; 2) uso de blindaje electromagnético para proteger los cables; 3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados unido a los cables; 4) acceso controlado a paneles de conexión y salas de cables (por ejemplo, con llaves mecánicas o PIN); 5) uso de cables de fibra óptica; d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable. Se debe buscar el asesoramiento de especialistas	Se cuenta con la seguridad en cableado estructurado	Teniendo en cuenta las pruebas adelantadas los días 20 y 21 de octubre de 2025, se observó que el cableado de las sedes de la Calle 26 y Calle 69 de la entidad no cuentan con la totalidad de los criterios requeridos en el control mencionado; es decir, que no se cuenta con: b.1) instalación de conductos blindados y cuartos o cajas cerradas y alarmas en los puntos de inspección y terminación; b.2) uso de blindaje electromagnético para proteger los cables; b.3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados unido a los cables; 4) acceso controlado a paneles de conexión y salas de cables (por ejemplo, con llaves mecánicas o PIN); 4.d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable. Adicionalmente a lo verificado, se observa que el área viene trabajando en un proyecto de cableado estructurado con PPTO Estimado: $140.000.000, con un inicio de identificación de cableado existente, organización y marcado como se observa en las fotos.		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
sobre cómo gestionar los riesgos derivados de incidentes o mal funcionamiento del cableado.		  Sin embargo, **se recomienda** al área que se estructure el plan de trabajo que permita evidenciar los avances obtenidos respecto a la organización que se viene desarrollando en pro del cumplimiento de las actividades relacionadas en el control. Este debe contener las actividades, las fechas de ejecución programadas, responsables, herramienta de medición, objetivo, fecha de elaboración, proyección de monitoreos periódicos y presentación de resultados al órgano competente (CIGD).		
A 7.14 / Eliminación segura o reutilización de equipos El equipo debe verificarse para asegurarse de que los medios de almacenamiento estén o no contenidos antes de su eliminación o eliminación. reutilizar. Los medios de almacenamiento que contengan información confidencial o con derechos de autor deben destruirse físicamente o la información debe destruirse, eliminarse o sobrescribirse utilizando técnicas para hacer que la información original no se	Se cuenta con la guía de borrado seguro	La entidad indica que se cuenta con la guía de borrado seguro, la cual se encuentra publicada en la intranet desde el 1 de noviembre de 2022, la cual **deberá** revisarse y actualizarse de conformidad con los lineamientos establecidos que contemple: 1. Medios de almacenamiento que contengan información confidencial o con derechos de autor deben destruirse físicamente o la información debe destruirse, eliminarse o sobrescribirse utilizando técnicas para hacer que la información original no se pueda recuperar en lugar de utilizar la función de eliminación estándar.		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
pueda recuperar en lugar de utilizar la función de eliminación estándar. Consulte 7.10 para obtener orientación detallada sobre la eliminación segura de medios de almacenamiento y 8.10 para obtener orientación sobre la eliminación de información. Las etiquetas y marcas que identifiquen a la organización o que indiquen la clasificación, el propietario, el sistema o la red deben eliminarse antes de su eliminación, incluida la reventa o la donación a organizaciones benéficas. La organización debe considerar la eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia, al final del contrato de arrendamiento o al mudarse de las instalaciones. Esto depende de factores como: a) su contrato de arrendamiento para devolver la instalación a su condición original; b) minimizar el riesgo de dejar los sistemas con información confidencial para el próximo inquilino (p. ej. listas de acceso de usuarios, archivos de video o imagen); c) la capacidad de reutilizar los controles en la siguiente instalación.		2. Etiquetas y marcas que identifiquen a la organización o que indiquen la clasificación, el propietario, el sistema o la red deben eliminarse antes de su eliminación, incluido el proceso de baja de la entidad. 3. Eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia, al final del contrato de arrendamiento o al mudarse de las instalaciones. Lo anterior, obedeciendo a la realidad de operación institucional, coordinación de lineamientos de operación de terceros respecto a controles de vigilancia, cumplimiento de las políticas de seguridad y privacidad, dando cabal cumplimiento a lo establecido en el control. **Respuesta al informe preliminar de auditoría:** Actualmente existe la Guía de Borrado Seguro, el control está implementado en su fase documental y el proceso de baja se coordina con el área de Recursos Administrativos. **Análisis Oficina de Control Interno:** La objeción no desvirtúa la observación, por lo tanto, esta **se mantiene:** Al señalar que el control está en “fase documental”, el propio proceso reconoce que: • La implementación no está cerrada. • Existen acciones pendientes de ejecución y registro. • La calificación del 100 % no es consistente con el estado real del control.		
A 8,8 / Gestión de vulnerabilidades técnicas	Se realiza gestión de vulnerabildades a traves de	Si bien el área cuenta con herramientas que permiten registrar y verificar la gestión de vulnerabilidades de		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
Identificación de vulnerabilidades técnicas La organización debe tener un inventario preciso de los activos (ver 5.9 a 5.14) como requisito previo para la gestión eficaz de la vulnerabilidad técnica; el inventario debe incluir el proveedor del software, el nombre del software, los números de versión, el estado actual de implementación (por ejemplo, qué software está instalado en qué sistemas) y la(s) persona(s) dentro de la organización responsable del software. Para identificar vulnerabilidades técnicas, la organización debe considerar: a) definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de vulnerabilidades, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidades, la actualización, el seguimiento de activos y cualquier responsabilidad de coordinación requerida; b) para el software y otras tecnologías (basado en la lista de inventario de activos, ver 5.9), identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles; c) exigir a los proveedores de sistemas de información (incluidos sus componentes) que garanticen la notificación, el manejo y la divulgación de vulnerabilidades, incluidos los requisitos de los contratos aplicables (véase 5.20); d) usar herramientas de escaneo de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y para verificar si el parcheo de vulnerabilidades fue exitoso (…)	herramientas que permiten su descubrimiento, asi mismo, realiza el segumiento sobre el avance de la subsanación https://lookerstudio.google.com/u/0/reporting/7ebb78ba-244c-4207-9993-955aa14dfeca/page/bic4E?s=lVkRlM2JF_0	conformidad con lo observado en las pruebas realizadas el 20 y 21 de octubre de 2025, no se dio el acceso de consulta de la herramienta al equipo auditor con el fin de efectuar el cruce de información entre las bases de datos y el visualizador de gestión de vulnerabilidades, así mismo, de conformidad con lo indicado en el control A 6.8 dentro de la base de datos no se encontró el registro de información de los correos maliciosos recibidos en múltiples ocasiones, así como tampoco la respuesta y gestión de los casos conocidos. Por lo anterior, se identifica una limitación al alcance en el marco de la evaluación; por lo que es importante que el área tenga en cuenta que se deben conceder los permisos de consulta a la totalidad de la información requerida por la Oficina de Control Interno, de conformidad con lo indicado en el numeral VIII del estatuto de auditoría de Canal Capital. De igual manera, **se recomienda** dar continuidad a la ejecución de pruebas planificadas periódicas, detección y gestión de incidentes, establecimiento de mejora continua. Así mismo, es importante que se otorguen los permisos requeridos por el equipo de auditor de manera que se puedan adelantar las revisiones requeridas y generar las recomendaciones pertinentes. **Respuesta al informe preliminar de auditoría:** Se cuenta con herramientas y gestión periódica para el descubrimiento, registro y seguimiento. El argumento de inexistencia de la información es desvirtuado con la evidencia de la gestión periódica y las herramientas de monitoreo como Fortigate, SOC, SIEM, Bitdefender, Dashboard de seguimiento de vulnerabilidades y Reportes de Colcert.		

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
		Análisis Oficina de Control Interno: Durante la auditoría **no se concedieron permisos de consulta** a las herramientas y tableros mencionados, lo cual impidió corroborar la información reportada, así como tampoco se concedieron los permisos en respuesta al informe preliminar de auditoría.		
A 8.23 / Filtrado web La organización debe reducir los riesgos de que su personal acceda a sitios web que contengan información ilegal o que se sepa que contienen virus o material de phishing. Una técnica para lograr esto funciona bloqueando la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware hacen esto automáticamente o pueden configurarse para hacerlo. La organización debe identificar los tipos de sitios web a los que el personal debe o no tener acceso. La organización debería considerar bloquear el acceso a los siguientes tipos de sitios web: a) sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas; b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing); c) servidores de mando y control; d) sitio web malicioso adquirido de inteligencia de amenazas (ver 5.7); e) sitios web que comparten contenido ilegal. Antes de implementar este control, la organización debe establecer reglas para el uso seguro y apropiado de los recursos en línea, incluida cualquier restricción a sitios web y aplicaciones basadas en la web	Se cuentan con políticas de filtrado web en el Firewall y en el Antivirus	Para dar cumplimiento a lo requerido en el control se establece por parte del área que se cuenta con: *Dos (2) equipos de seguridad perimetral (firewall) para controlar el flujo de información que entra y sale a través de internet a la entidad – limitación del tráfico a través de los puertos. IP pública (Intranet), mesa de servicio (futuro) y control de consumo de elementos (misionales). Monitoreo diario del consumo, se realiza análisis con reporte Fortigate – 1. Bloqueo, 2. Tráfico (Directivo) técnico con D. Operativa* *• Antivirus – detección del tipo de vulnerabilidad, reporte diario y mensual generado por el proveedor.* *• Vulnerabilidades – Dashboard, acta de reunión quincenal en la cual se revisan.* De conformidad con los resultados verificados durante las pruebas del 20 y 21 de octubre de 2025, se cuenta con monitoreo de acceso al tráfico de páginas web, información y gestión con los supervisores sobre el acceso a contenidos y páginas que no estén permitidas en la ejecución de las obligaciones de los contratistas. Sin embargo, **se recomienda** que se efectúe la documentación que permite contar con la trazabilidad del trámite ejecutado en reuniones de tráfico con los supervisores, así como de gestión del área.	**x**	

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
indeseables o inapropiados. Las reglas deben mantenerse actualizadas.				
A 8.30 / Desarrollo subcontratado Cuando se subcontrata el desarrollo del sistema, la organización debe comunicar y acordar los requisitos y expectativas, y monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con estas expectativas. Se deben considerar los siguientes puntos en toda la cadena de suministro externa de la organización: a) acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el subcontratado contenido (ver 5.32); b) requisitos contractuales para prácticas seguras de diseño, codificación y pruebas (véanse 8.25 a 8.29); c) provisión del modelo de amenaza a considerar por desarrolladores externos; d) pruebas de aceptación para la calidad y exactitud de los entregables (ver 8.29); e) provisión de evidencia de que los niveles mínimos aceptables de seguridad y capacidades de privacidad son establecidos (por ejemplo, informes de aseguramiento); f) provisión de evidencia de que se han realizado suficientes pruebas para proteger contra la presencia de contenido malicioso (tanto intencional como no intencional) en el momento de la entrega; g) provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas; h) acuerdos de depósito en garantía para el código fuente del software (por ejemplo, si el proveedor cierra); i) derecho contractual a auditar procesos y controles de desarrollo;	No aplica	Se indica por parte del área que el control no aplica siendo calificado al 100%; sin embargo, es importante que se tenga en cuenta que la suscripción de contratos por prestación de servicios para desarrollo es una manera de subcontratación, dado que **no** hay personal de planta de la entidad realizando ese tipo de actividades, lo que se denota en las obligaciones específicas de las personas vinculadas al área de Tecnologías de la Información y las comunicaciones las cuales indican: * *Apoyar en el diseño, **desarrollo** y mantenimiento de aplicaciones bajo principios de integración continua y entrega continua (CI/CD), así como pruebas automatizadas, asegurando versiones estables, seguras y confiables.* * *Apoyar al área de Gestión TIC en la implementación y mantenimiento de prácticas de seguridad en el ciclo de vida del desarrollo (DevSecOps), incorporando revisiones de código seguro, análisis y gestión de vulnerabilidades y controles de cumplimiento normativo.* Adicionalmente, respecto a los requisitos de ejecución del control el área deberá establecer: * Acuerdos de propiedad del código y derecho de propiedad intelectual del desarrollo * Complementar los requisitos contractuales para prácticas seguras del diseño, creación, codificación y pruebas de conformidad con las obligaciones contractuales relacionadas en las minutas * Determinar el modelo de amenazas a considerar por el desarrollo de externos (riesgos), así como de pruebas de calidad a los productos requeridos y pruebas de protección de contenidos malicioso.		**x**

Control / Descripción / Evidencia de cumplimiento del control solicitada por el MSPI	Evidencia reportada en el autodiagnóstico del 1 de ene de 2024 al 30 jun de 2025	Observaciones/ Recomendaciones verificación OCI	¿Se concluye una calificación de implementación del 100?	
			SI	NO
j) requisitos de seguridad para el entorno de desarrollo (ver 8.31); k) teniendo en cuenta la legislación aplicable (por ejemplo, sobre protección de datos personales).		* Auditoría a los procesos y controles del desarrollo, requisitos de seguridad (protección de datos) con personal que cuente con el conocimiento en materia de la norma 27001 Lo anterior, dado que, dentro de la documentación del área, así como de los contratos suscritos no se observa que se cuente con información que permita determinar la ejecución integral de los criterios del control. Es importante que se tenga en cuenta que las políticas deben ser definidas de manera clara, comunicarlas, revisarlas, actualizarlas, ejercer ejercicios de retroalimentación y mejora continua. Por lo anterior, **se recomienda** la revisión del control, así como la recalificación y definición de actividades para el cumplimiento del 100% de lo requerido en la norma. **Respuesta al informe preliminar de auditoría:** El control se calificó como "No Aplica" debido a que los contratos son de apoyo a funciones de personal de planta, cuyas obligaciones ya contemplan las prácticas de seguridad (DevSecOps). Se acoge la recomendación de recalificación y fortalecimiento de las cláusulas contractuales como una mejora para la formalización en la transición, dado el nuevo enfoque de la Resolución 02277. **Análisis Oficina de Control Interno:** Teniendo en cuenta lo indicado por el área **se mantiene** la observación.		

Como síntesis de lo presentado en la Tabla 1, se observa que se presentan:

A. Inconsistencias en el reporte de información del autodiagnóstico del MSPI al no presentarse completitud en su diligenciamiento.

Durante la revisión se evidenció que, aunque los controles presentan descripciones amplias y detalladas en su formulación (primera columna de la tabla 1), los registros aportados por el área en el autodiagnóstico son generales e incompletos; es decir, no abarcan la totalidad de los elementos exigidos por cada control de la herramienta respecto a la medición de avances de implementación del MSPI. Esta situación limita la confiabilidad del reporte y no refleja de manera precisa el estado real de implementación al interior de Canal Capital.

Respuesta al informe preliminar de auditoría:

El autodiagnóstico refleja la existencia y aplicabilidad del control. La totalidad de la evidencia solicitada, que soporta la gestión de los controles, fue entregada al equipo auditor dentro del alcance temporal (10/2024 - 07/2025). La inconsistencia en el reporte hace parte del proceso de transición y articulación con el nuevo modelo según la Resolución 02277, pero no desvirtúa la aplicación del control durante el periodo auditado.

Análisis Oficina de Control Interno:

La objeción no desvirtúa la observación, por lo cual esta **se mantiene**, por las siguientes razones técnicas:

- El alcance de la observación no es la inexistencia del control, sino la calidad del autodiagnóstico, La observación no cuestiona que existan controles ni que se hayan ejecutado actividades durante el periodo auditado. Tal como se deja explícito en el informe preliminar, la observación se fundamenta en que:

  - El autodiagnóstico del MSPI es el instrumento oficial de medición y reporte definido por MinTIC (Resolución 2277 de 2025), en dicho instrumento, los registros son generales, incompletos o no abarcan la totalidad de los requisitos del control, pese a que posteriormente se aportaron evidencias adicionales durante la auditoría.

  - Se evidencia una brecha entre lo reportado y lo evidenciado, lo que afecta la confiabilidad del autodiagnóstico como herramienta de gestión y toma de decisiones, independientemente de que existan soportes.

B. Desarticulación de las áreas responsables de implementación de controles transversales del MSPI.

Si bien la responsabilidad de la implementación del MSPI en Capital recae formalmente en el área de Gestión TIC, en el autodiagnóstico no se evidencia de manera clara cómo este proceso se articula con las áreas que también tienen controles a su cargo, particularmente Servicios Administrativos, Contratación, Jurídica y Talento Humano. Este es el caso de los controles: A 5.34, A 6.6, A 7.1 y A 7.6.

De igual manera, no se observa reporte y evidencia en el autodiagnóstico que muestre que Gestión TIC haya orientado, informado o comunicado formalmente a estas áreas sobre:

- Los controles específicos bajo su responsabilidad, requisitos, recomendaciones de implementación y monitoreo de avances.

- Los insumos y reportes que deben registrarse en la herramienta del MSPI. (estas áreas deberían reportar en el autodiagnóstico, o reportar al área de Gestión TIC cómo se da cumplimiento al control).

- Los mecanismos de seguimiento periódico por parte del área de Gestión TIC para verificar su avance, cumplimiento o brechas.

- Comunicación a la Alta Gerencia sobre los avances efectivamente alcanzados o rezagos identificados para la toma de decisiones sobre aspectos que puedan llegar a afectar la misionalidad de la entidad, así como el establecimiento de necesidades de operación que atiendan a la realidad institucional.

Respuesta al informe preliminar de auditoría:
La articulación existe y se formaliza mediante documentos y procesos interinstitucionales que aplican los controles transversales: Contratación/TH (cláusulas de confidencialidad y PI), Servicios Administrativos (seguridad física, A.7.1). El autodiagnóstico refleja la responsabilidad principal de Gestión TIC, pero la ejecución de controles transversales está cubierta por soportes formales que demuestran la sostenibilidad del MSPI dentro del periodo 10/2024 - 07/2025; de igual forma los avances, documentos, políticas, procedimientos entre otros relacionados al Modelo son presentados para aprobación y/o socialización ante el Comité Institucional de Gestión y Desempeño según aplique y en mismo participan las áreas misionales y de apoyo.

Análisis Oficina de Control Interno:
La objeción no desvirtúa la observación, por lo tanto esta **se mantiene**, se describen las siguientes razones técnicas:

- La observación no desconoce la existencia de cláusulas contractuales, políticas, procedimientos o actividades operativas en otras áreas. Como se indica en el informe, los controles transversales fueron reportados por Gestión TIC en el autodiagnóstico sin insumos formales (reportes, actas de seguimiento, matrices de responsabilidades) provenientes de Jurídica, Talento Humano, Servicios Administrativos o Contratación.

- La existencia de cláusulas o políticas no se tradujo en registros estructurados dentro del instrumento de autoevaluación, por el contrario, toda la información indicada no es reportada en el autodiagnóstico, lo anterior afecta la confiabilidad y confirma la desarticulación señalada.

C. Inexistencia de un plan de trabajo o documento equivalente que contemple la totalidad de requisitos para implementación de los controles del MSPI, que permita soportar el cumplimiento registrado en la herramienta de "Controles organizacionales".

Teniendo en cuenta que se tomó una muestra de (20) controles, se observó que en varios de estos se reportó un cumplimiento del 100% aun cuando la verificación permitió identificar que no se ejecutan o no se documentan todos los componentes del control, de conformidad con el requisito técnico normativo. Esto sugiere que la calificación otorgada por el proceso no corresponde al nivel real de implementación y evidencia una brecha en la autoevaluación realizada. Este es el caso de los controles: A 5.3, A 5.7, A 5.19, A 5.32, A 5.37, A 6.6, A 6.3, A 6.8, A 7.1, A7.6, A 7.7, A 7.12, A 7.14, A 8.8 y A 8.30.

En general se evidencia la necesidad de establecer un plan de acción formal, con periodos de monitoreo definidos (semestral o anual, teniendo en cuenta la condición del autodiagnóstico), que permita priorizar las brechas identificadas y determinar qué controles del MSPI serán abordados en cada corte. Este plan debe incluir responsables, actividades, plazos, ponderaciones, recursos requeridos y criterios de seguimiento.

Asimismo, es necesario implementar un mecanismo de monitoreo y reporte periódico que evidencie el avance en la implementación de los controles pendientes, el cierre progresivo de brechas y la efectividad de las acciones ejecutadas. Esto garantizará continuidad, trazabilidad y oportunidad en el proceso de implementación del MSPI al interior de Canal Capital.

Respuesta al informe preliminar de auditoría:
La calificación del 100% obtenida en el autodiagnóstico de la herramienta de "Controles Organizacionales" se fundamenta en la existencia, aprobación y aplicación efectiva de la documentación base del Modelo de Seguridad y Privacidad de la Información (MSPI) (Políticas, Guías y Procedimientos), lo cual constituye el objetivo primordial del MSPI durante su fase de implementación y sostenibilidad, y que fue aprobado y socializado

ante el CIGD. Respecto a la presunta inexistencia de un plan de trabajo o documento equivalente que soporte dicho cumplimiento, es importante señalar que el Plan de Trabajo estructurado es la hoja de ruta para la gestión y cierre de brechas de seguridad, la cual se integra en el Plan de Mejoramiento. Este plan fue puesto a disposición y se acordó su análisis por el equipo auditor, lo que demuestra la gestión activa en la transición, tal como quedó consignado en el Acta del 29/08/2025. Adicionalmente, se aclara que, en la medición del autodiagnóstico, aquellos controles que han sido formalmente definidos como “No Aplicables” a la operación de Canal Capital se reportan con un cumplimiento del 100%. Esta metodología fue adoptada debido a que el instrumento de medición actualmente utilizado no contempla la opción de “No Aplica”; asignar un valor de 0% a estos controles resultaría en una distorsión a la baja de la medición general del cumplimiento del instrumento.

Análisis Oficina de Control Interno:
La objeción no desvirtúa la observación y esta **se mantiene**, por las siguientes razones:

- El informe preliminar reconoce la documentación existente; por lo que la observación se formula dado que no se evidenció un instrumento de monitoreo y cierre de brechas de los controles evaluados en cero o en proceso de implementación.

- El Plan de Mejoramiento no sustituye o equivale a un plan de implementación y sostenibilidad del MSPI, el cual es requerido para soportar el avance de Capital en el cierre de brechas y mantenimiento de todos los controles con una calificación por debajo de 100%.

- No se evidenció que, al momento del autodiagnóstico, existiera un plan de trabajo vigente que permita determinar para un periodo de tiempo que acciones se están implementado para cumplir con los controles que apliquen a Capital.

- La presentación de documentos ante el CIGD hace parte de la ejecución del Plan de trabajo y con el fin de establecer su nivel de avance se requiere de un plan estructurado de implementación y seguimiento.

13. OBSERVACIONES

N°	Observaciones	¿Requiere valoración de riesgo?	Área[1]
1	**DESCRIPCIÓN:** Debilidades en el diligenciamiento del autodiagnóstico del MSPI, debido a:	**No**	**TIC**

[1] Área o áreas responsables de adelantar la formulación de la(s) acción(es) que se consideren pertinentes.

N°	Observaciones	¿Requiere valoración de riesgo?	Área[1]
	a) Inconsistencias y falta de completitud en las evidencias que demuestren el cumplimiento integral de todo lo solicitado en el control. b) Desarticulación en el diligenciamiento del autodiagnóstico con las áreas responsables de los controles transversales evaluados del MSPI **CRITERIO DE AUDITORÍA:** • Instrumento de Autoevaluación del MSPI de enero a junio de 2025. • Resolución 2277 de 2025 del MinTic		
2	**DESCRIPCIÓN:** Inexistencia de un plan de trabajo o documento equivalente que contemple la totalidad de requisitos para implementación de los controles del MSPI, que permita soportar el cumplimiento registrado en la herramienta de "Controles organizacionales". **CRITERIO DE AUDITORÍA:** • Instrumento de Autoevaluación del MSPI de enero a junio de 2025. • Resolución 2277 DE 2025 del MinTic	**No**	**TIC**
Total observaciones		**2**	

14. CONCLUSIONES

Se cumplió el objetivo de la auditoría verificando la implementación de los controles del Modelo de Seguridad y Privacidad de la Información (MSPI) en Capital, contrastando la información reportada en el autodiagnóstico con las evidencias documentales y las pruebas en campo. Así mismo se destacan avances como:

13.1. La entidad ha desarrollado documentos, guías y procedimientos relevantes en materia de seguridad de la información; sin embargo, presentan debilidades en su formalización, actualización y socialización.

13.2. Se consolidan avances en la ejecución y registro de cumplimiento de cinco (5) controles de los (20) evaluados, destacando actividades de derechos de acceso, incidentes de seguridad, privacidad y protección de datos personales, términos y condiciones del empleo y filtrado web.

De igual manera, se hace necesario que se adelanten acciones respecto a las debilidades identificadas en el marco de:

13.3. El análisis evidenció inconsistencias entre los niveles de cumplimiento reportados (calificados en su mayoría al 100 %) y la evidencia realmente disponible. También se evidencian aspectos que robustecen el reporte que no son incluidos.

13.4. Aunque la responsabilidad sobre la implementación del MSPI está asignada al área de Gestión TIC, no se evidencia un esquema formal de coordinación con otras áreas tales como Jurídica, Talento Humano, Servicios Administrativos y Contratación, pese a que estas áreas son responsables directas de varios controles. No se observa acompañamiento, directrices ni seguimiento respecto a lo que cada dependencia debe reportar en la herramienta del MSPI.

13.5. Falta la socialización periódica de los diferentes lineamientos en materia de escritorio y pantalla despejados, al igual que políticas complementarias definidas para la entidad, el programa de capacitación (articulado con el área de Talento Humano).

13.6. Se cuenta con debilidades en el registro de información sobre la gestión de incidentes al no tener la totalidad de información requerida por el control, así como del registro de la información entregada por las áreas.

13.7. No se cuenta con una base de datos y/o registro documentado de las acciones de borrado y/o eliminación para reutilización o baja de equipos que permita registrar de manera adecuada la implementación del control establecido en la entidad.

15. RECOMENDACIONES

15.1. Fortalecer el autodiagnóstico del MSPI: Ajustar el diligenciamiento del instrumento para garantizar consistencia, completitud y trazabilidad entre la calificación asignada y la evidencia disponible, evitando sobreestimaciones del nivel real de implementación de los controles.

15.2. Alinear la calificación de controles con su estado real: Definir criterios internos de autoevaluación que diferencien controles documentados, parcialmente implementados y plenamente operativos, reflejando adecuadamente las brechas existentes.

15.3. Formalizar un plan de trabajo del MSPI: Formular y adoptar un plan de trabajo específico del MSPI que articule controles, brechas, actividades, responsables,

cronograma e indicadores, independiente del Plan de Mejoramiento derivado de auditorías.

15.4. Establecer un mecanismo documentado de coordinación y reporte con las áreas responsables de controles transversales, asegurando insumos formales y seguimiento periódico dentro del MSPI.

15.5. Formalizar los documentos clave del MSPI en el Sistema Integrado de Gestión, garantizando aprobación, control de versiones, vigencia y accesibilidad institucional.

15.6. Implementar programas periódicos y medibles de concientización, capacitación y entrenamiento en seguridad de la información, con enfoque institucional y evaluación de eficacia.

15.7. Asegurar a la Oficina de Control Interno el acceso oportuno a la información y herramientas del MSPI, conforme al Estatuto de Auditoría, evitando limitaciones al alcance.

Revisó y aprobó:

NESTOR FERNANDO AVELLA AVELLA

Firmado digitalmente por: NESTOR FERNANDO AVELLA AVELLA
Serial del certificado: 59db216353dc996c
Entidad: CANAL CAPITAL
Unidad Organizacional: CONTROL INTERNO
Cargo: JEFE CONTROL INTERNO
Localizacion: BOGOTA
Fecha y hora: 2025-12-23T12:15:11.855-05:00

Jefe Oficina de Control Interno

Preparó: Diana del Pilar Romero Varila, Contratista Oficina de Control Interno – Cto. 037-2025
Jizeth Hael González Ramírez, Contratista Oficina de Control Interno – Cto. 006-2025