TIPO DE INFORME:	Preliminar		Final	x

Tabla de contenido

Índice de tablas

Índice de gráficos

1. TÍTULO DE LA AUDITORÍA

Auditoría a las normas de Gestión: Sistemas de Gestión de Seguridad y Salud en el trabajo - SGSST y Norma ISO 27001: Seguridad de la Información.

2. FECHA DE LA AUDITORÍA

Del 01 de abril al 31 de agosto de 2023.

3. PERIODO EVALUADO

Del 01 de enero de 2022 al 31 de marzo de 2023.

4. PROCESO AUDITADO

ISO 27001:2013, Modelo de Privacidad y Seguridad de la Información.

5. LÍDER DEL PROCESO / LÍDER DEL ÁREA

Uriel de Jesús Bayona Chona – Subdirector Administrativo / Mauris Antonio Ávila – Profesional especializado de Sistemas.

6. AUDITORES

Diana del Pilar Romero Varila / Jizeth Hael González Ramírez.

7. OBJETIVO DE LA AUDITORÍA

Verificar el cumplimiento de la implementación de la norma de gestión ISO 27001:2013 en Capital.

8. ALCANCE DE LA AUDITORÍA

Abarca las actividades ejecutadas para la implementación de la norma de gestión ISO 27001:2013 en Capital para el periodo comprendido entre el 1 de enero de 2022 al 31 de marzo de 2023.

Limitación al alcance: Teniendo en cuenta que en el equipo de Control Interno no se cuenta con un Ingeniero de Sistemas o profesional con carreras afines, se limitó la verificación de los controles de la ISO 27001 de conformidad con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información – MSPI dado el conocimiento técnico que se requiere para identificar y verificar su adecuado cumplimiento e implementación en Capital.

9. CRITERIOS

Generales:

- 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".
- Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG - Versión 4 - marzo 2021.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6.

MPSI – ISO 27001:

- NTC ISO 27001:2013
- Resolución 500 de 2021 del Ministerio de las TIC, "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".
- 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.

- Caracterización, procedimientos, formatos, manuales y políticas del proceso de Gestión de Recursos Administrativos - Sistemas y demás normatividad vigente aplicable.
- 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.

10. 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), concordante con los lineamientos señalados en la norma ISO 19011-2018 y demás lineamientos establecidos al interior de Capital para el ejercicio de la auditoría interna, 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 del área y elaboración del Plan de Auditoría Individual [CCSE-FT-012].
- Definición del objetivo, alcance, riesgos, recursos y programa de trabajo.
- Preparación de papeles de trabajo de la revisión documental y procedimental sobre la unidad auditada, así como las actividades con procesos adyacentes como Gestión de recursos administrativos y Gestión del Talento Humano.
- Preparación de solicitudes de información a la unidad auditada y áreas adyacentes del proceso.

Ejecución

- Solicitud de información mediante correos electrónicos y memorando 459 del 16 de junio de 2023.
- Revisión documental de la unidad auditable como la caracterización, formatos, manuales y procedimientos asociados a la implementación del modelo de privacidad y seguridad de la información – ISO 27001.
- Prueba de recorridos Sede calle 26 (16 de agosto) y calle 69 (24 de agosto)
- Entrevista a los Profesionales de Sistemas el 16 de agosto de 2023.
- Análisis de la información remitida (soportes) por las unidades auditables, en herramienta digital (Drive), información tomada durante las pruebas de recorrido, así como de correos electrónicos, con el fin de validar el cumplimiento de las disposiciones legales vigentes y demás normas aplicables en materia de ISO 27001 – Modelo MSPI.
- Teniendo en cuenta que la implementación de todos los requisitos de cada una de las cinco fases son la base para la correcta implementación del MSPI, así como de los controles seleccionados, se procedió a verificar el nivel de implementación de estos lineamientos en Capital, para lo cual se establecieron los siguientes parámetros de calificación:

  1-Inexistente, no existen actividades diseñadas para cubrir el requerimiento.
  2-Documentado, existen actividades en proceso de diseño o están diseñadas pero se evidencian oportunidades de mejora.
  3-Implementado, actividades diseñadas, documentadas y socializadas de acuerdo con el requerimiento.

Informe de Auditoría

- Consolidación y entrega del informe preliminar de auditoría a los líderes y/o responsables de los procesos auditados en el formato CCSE-FT-016.
- Análisis de las respuestas remitidas por los líderes de proceso y equipos de trabajo frente a las observaciones señalas en el informe preliminar.
- Consolidación y entrega del informe final de auditoría a la Gerente, líderes y/o responsables de la unidad auditable y procesos adyacentes evaluados, en los formatos dispuestos para tal fin [CCSE-FT-016] y [CCSE-FT-024].

Seguimiento del progreso

- Solicitud de la formulación del Plan de Mejoramiento en el formato CCSE-FT-001 frente a las actividades que eliminen las causas de las observaciones encontradas.
- Acompañamiento de la formulación del Plan de Mejoramiento al área.
- Análisis de la evaluación de la auditoría CCSE-FT-018 y presentación al Comité Institucional de Coordinación de Control Interno para implementación de mejoras en el ejercicio de auditoría.

11. RESULTADOS DEL TRABAJO DE AUDITORÍA

11.1. ASPECTOS POSITIVOS

- Capital durante el periodo evaluado implementó y actualizó lineamientos: Guías, manuales y planes requeridos para la implementación y mejora del Modelo de seguridad y Privacidad de la Información - MSPI.
- El área de Sistemas adelantó la autoevaluación del Modelo de Seguridad y Privacidad de la Información en la herramienta determinada por MinTic.
- Se identificaron riesgos de seguridad digital, y se implementó y adoptó la matriz en la entidad.
- Se realizaron capacitaciones a los colaboradores de la entidad, en temas relacionados con el MSPI.
- Hay compromiso desde la Dirección de la entidad para la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, de conformidad con las responsabilidades asignadas al CIGD.
- Se ha mejorado el respaldo eléctrico antes cortes de energía en las Sedes de la Calle 26 y la Casa de la 69.
- Se establecen lineamientos a nivel institucional para verificar la idoneidad de los colaboradores que ingresaran a Capital y que dentro de sus funciones u obligaciones contractuales tienen el control de acceso a la información de Capital.
- Se restringe el acceso a sitios externos para reducir la exposición a contenido malicioso, sin embargo, debe establecerse una política para realizar este tipo de restricciones.
- Se ha promovido el desarrollo de software in-house, para atender las necesidades específicas de las diferentes áreas de Capital.
- Se cuentan con entornos separados de pruebas y producción para el desarrollo de software.
- Se evidencia la asignación de recursos financieros y humanos a través del proyecto de inversión 7511"Fortalecimiento de la capacidad administrativa y tecnológica para la gestión institucional de Capital" de Capital, para implementar y mejorar el modelo MSPI.

11.2. AUTODIAGNÓSTICO DEL MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN - MSPI

De conformidad con los lineamientos del MinTic, las entidades deben aplicar la herramienta de autodiagnóstico (Análisis GAP), con el propósito de establecer el estado actual de la entidad respecto a la Seguridad y privacidad de la Información y de conformidad con los resultados establecer acciones de mejoramiento continuo.

Capital realizó en noviembre de 2022 una actualización del diagnóstico, obteniendo un resultado promedio de 85% en la implementación de controles, dando como resultado en la escala de valoración el modelo como "Gestionado", de conformidad con este resultado el modelo tendrá oportunidades de mejora y la implementación acciones de mejora, como se indica en la herramienta:

Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.

Fuente: Escala de valoración de controles herramienta de autodiagnóstico (Análisis GAP)

La OCI procedió a verificar aleatoriamente las evidencias y la información reportada por el área de Sistemas para soportar el nivel de cumplimiento de los controles en la herramienta, evidenciando las siguientes debilidades a nivel general en el registro de información:

a. Hay casos donde no se reporta un nivel de cumplimiento del 100%, y no se indica cuál es la debilidad o brecha de Capital para cumplir con el requisito normativo, ni se indica cuál es la evidencia que soporta el porcentaje de cumplimiento indicado, ni la recomendación o mejora que se establecerá:

Ilustración 1. Cumplimiento controles - MSPI.

ITEM	DESCRIPCIÓN	ISO	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	A.6.1.2			80	

ITEM	DESCRIPCIÓN	ISO	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	A.9.2.4	Minutas contratuales y manual de funciones		80	Todo el proceso de confidencialidad y responsabilidad se realiza a través de la minuta contractual y funciones al personal de la entidad.

b. En este ítem se califica como "no aplica" para Capital, sin embargo existen documentos al interior de la entidad que dan cuenta de la necesidad de su aplicación, adicional en el reporte no se indicó el criterio técnico por el cual no es aplicable este requisito.

Ilustración 2. Modelo MSPI - Calificado N/A

ITEM	DESCRIPCIÓN	ISO	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
Reglamentación de controles criptográficos.		A.18.1.5			n/a	

c. Hay casos dónde se indica que no se cumple con el control establecido, pero se califica con un porcentaje de cumplimiento avanzado, sin aclarar si hay otras evidencias que permitan soportar el porcentaje de avance indicado:

Ilustración 3. Modelo MSPI - Calificado No cumple

ITEM	DESCRIPCIÓN	ISO	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7			60	No se cuenta con el procedimiento documentado.

ITEM	DESCRIPCIÓN	ISO	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
CRIPTOGRAFÍA	**Marco de referencia de gestión para iniciar y controlar la implementación**	**A.10**			20	
CONTROLES CRIPTOGRÁFICOS	**Asegurar el uso apropiado y eficaz de la criptografía para proteger la**	**A.10.1**			20	
Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles	A.10.1.1			20	No se cuenta con un documento que de cuenta de la politica.
Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves	A.10.1.2			20	

Por lo anterior, es importante que se revise y complemente la información reportada diligenciando todas las columnas de la herramienta las cuáles permiten evidenciar cómo se cumple el requisito, sino se está cumpliendo, qué brechas existen y cuáles recomendaciones se implementarán para su cumplimiento, y en el caso dónde no aplican requisitos normativos explicar los motivos por los cuáles no se implementan en Capital.

11.3. DOCUMENTO MAESTRO DEL MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN (MSPI)

Como se menciona en la metodología, teniendo en cuenta que la implementación de todos los requisitos de cada una de las cinco fases son la base para la correcta implementación del MSPI, se procedió a verificar el nivel de implementación de estos lineamientos en Capital, para lo cual se establecieron los siguientes parámetros de calificación:

- 1 - Inexistente, no existen actividades diseñadas para cubrir el requerimiento.
- 2 - Documentado, existen actividades en proceso de diseño o están diseñadas pero se evidencian oportunidades de mejora.
- 3- Implementado, actividades diseñadas, documentadas y socializadas de acuerdo con el requerimiento.

MinTic mediante el documento maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf estableció los lineamientos generales para formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información[1] Diagnóstico, planificación, operación, evaluación del desempeño y mejoramiento continuo.

Los ítems que tengan calificación de 1 y 2 requerirán la formulación de acciones de mejora. Una vez evaluadas las cinco fases del lineamiento, se obtuvieron los siguientes resultados:

[1] Tomado de la introducción del documento maestro del MSPI de octubre de 2021

Tabla 1. Cumplimiento lineamientos del documento maestro del MSPI

CAPITAL, SISTEMA DE COMUNICACIÓN PÚBLICA
OFICINA DE CONTROL INTERNO

PAPEL DE TRABAJO	
Auditoría:	Auditoría a las normas de Gestión: Sistemas de Gestión de Seguridad y Salud en el trabajo - SGSST y Norma ISO 27001: Seguridad de la Información.
Periodo evaluado:	1 de enero de 2022 al 31 de marzo de 2023.
IDENTIFICACIÓN DE LA ACTIVIDAD	
Tipo de evaluación:	Implementación de lineamientos y controles de la ISO 27001:2013
Auditor(es) responsable(s):	Jizeth González / Diana Romero
Fecha ejecución:	jun-23
Objetivo:	Verificar el nivel de implementación de los lineamientos establecidos en el Documento Maestro del Modelo de Privacidad y Seguridad de la Información: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

7.	FASE DE PLANIFICACIÓN			
7.1.	**CONTEXTO**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
7.1.1	Comprensión de la organización y de su contexto	Contexto de la entidad (Política de Planeación Institucional)	**2**	Capital cuenta con la Política de Planeación Institucional [EPLE-PO-004] aprobada el 02/11/2022 por el Comité Institucional de Gestión y Desempeño; sin embargo, no se evidencian aspectos del modelo de procesos y servicios, de conformidad con los lineamientos de arquitectura definido por MinTic. Por lo cual, es pertinente revisar la política con el área de Planeación y complementar esta, teniendo en cuenta el marco de Referencia de Arquitectura Empresarial definido por MinTIC [].
7.1.2	Necesidades y expectativas de los interesados	Partes interesadas (Política de Planeación Institucional)	**2**	Capital cuenta con la Política de Planeación Institucional [EPLE-PO-004] aprobada el 02/11/2022 por el Comité Institucional de Gestión y Desempeño; sin embargo, no se evidencian de manera clara la identificación de necesidades y expectativas de las partes interesadas internas y externas que influyen directamente en la seguridad de la información de Capital o que puedan verse afectados en caso de que estas se vean comprometidas. Por lo cual, es pertinente revisar la política con el área de Planeación e identificar de manera clara las partes interesadas del MSPI (necesidades y expectativas)
7.1.3	Definición del alcance del MSPI	Alcance (Modelo de Planeación y Gestión)	**2**	Se indica por parte del área: *"en el plan de seguridad y privacidad de la información se encuentra contemplado el Modelo de Seguridad y Privacidad de la Información-MSPI"*; sin embargo, teniendo en cuenta el requisito normativo, dicho alcance debe documentarse en Manual del Sistema Integrado de Gestión, una vez verificado el documento de Capital denominado EPLE-MN-004 Manual del MIPG no se observa la definición de dicho alcance, así como tampoco la mención o relación de lo requerido, ya que, se menciona el requisito general de implementar lineamientos de Gobierno Digital. Con base en lo anterior, se adelantó la evaluación de la documentación de dichos requisitos en materia de arquitectura empresarial, evidenciando su mención en el Plan Estratégico de Tecnologías de la Información-PETI 2021-2024, por lo que se establece la necesidad de modificar lo documentado en el Manual, articulando la información del PETI de manera que se dé cumplimiento a lo requerido indicando las necesidades, modelo de procesos, recursos necesarios para la implementación, presupuesto y sedes físicas. Lo anterior, aterrizado a la realidad de Capital.
7.2.	**CONTEXTO**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
7.2.1	Liderazgo y compromiso	Acto administrativo de conformación del Comité de Gestión y Desempeño (Funciones de Seguridad y Privacidad de la información)	**3**	Acto administrativo: Resolución 081-2021 en el cual se define la responsabilidad de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, en el artículo 8.
7.2.2	Política de seguridad y privacidad de la información	Acto administrativo de adopción de la Política de seguridad y	**1**	Se cuenta con la Política de seguridad y privacidad de la información [AGRI-SIPO-002] aprobada por el Comité Institucional de Gestión y Desempeño del

		privacidad de la información.		24/09/2020. Sin embargo, no se evidencia acto administrativo de adopción de esta. Lo anterior, de conformidad con lo indicado por el Consejo de Estado, respecto a que: *"el acto administrativo es toda manifestación de voluntad de una entidad pública, o de un particular en ejercicio de funciones públicas, capaz de producir efectos jurídicos"* y por lo tanto, el acta de dicho Comité y el documento que contiene la Política no puede entenderse como un acto administrativo [con lo cual se dé cumplimiento al requerimiento].
7.2.3	Roles y responsabilidades	Definición de roles y responsabilidades.	**2**	Se identifican en el numeral 7 de la Política de seguridad y privacidad de la información [AGRI-SIPO-002] aprobada por el Comité Institucional de Gestión y Desempeño el 24/09/2022. Sin embargo, se identifican debilidades teniendo en cuenta que no se evidencian responsabilidades en materia de ciberseguridad y T.I., de igual manera, estás no guardan coherencia con la política de administración del riesgo, y a la realidad de la entidad teniendo en cuenta que el Comité Institucional de Gestión y Desempeño no actualiza y presenta la metodología para el análisis de riesgos, de conformidad con lo indicado en el artículo 5 de la Resolución 081 de 2021 es función del Comité aprobar la política, así mismo teniendo en cuenta lo formulado en la Política de Administración del riesgo es responsabilidad de la segunda línea definir la metodología de administración del riesgo
7.3.	**PLANIFICACIÓN**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
7.3.1	Identificación de activos de información e infraestructura crítica.	* Procedimiento de inventario y clasificación de la información. * Documento metodológico del inventario y clasificación de la información.	**1**	Si bien se cuenta con un inventario y clasificación de información, no se cuenta con un procedimiento de inventario y clasificación de información, así como tampoco se cuenta con documento metodológico que permita adelantar el inventario y clasificación de la información generada por Capital.
7.3.2	Valoración de los riesgos de seguridad de la información	* Procedimiento y metodología de gestión de riesgos institucional, aprobado por el CICCI.	**2**	Capital cuenta con Política de administración de riesgos aprobada por el Comité Institucional de Coordinación de Control Interno - CICCI y Manual de administración del riesgo aprobados durante diciembre de 2022. Sin embargo, debe revisarse las calificaciones del nivel de probabilidad e impacto, ya que difieren de las aprobadas en la política de administración del riesgo, de conformidad con lo indicado en el numeral 11.7
7.3.3	Plan de tratamiento de los riesgos de seguridad de la información	* Plan de tratamiento de riesgos aprobado por el CIGD (Dec. 612-2018) * Declaración de aplicabilidad aceptada y aprobada por el CIGD.	**1**	Se identifica el *"Plan de tratamiento de riesgos de seguridad y privacidad de la información"* dentro del Plan de Acción de la vigencia 2023 con fecha del 31/01/2023 en el cual se identifica una (1) actividad, la cual no es coherente con lo requerido en el plan de tratamiento, al no identificarse las acciones de gestión de los riesgos dependiendo de la zona en la que se ubica; lo anterior, ya que la acción se formula para monitoreo de riesgos de seguridad digital con un indicador de "Matriz de riesgos de seguridad digital". No se evidencia aprobación del CIGD del plan de tratamiento de riesgos CÓDIGO: AGRI-SI-PL-004, ni de la "Declaración de aplicabilidad" aceptada y aprobada por el CIGD.
7.4.	**SOPORTE**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
7.4.1	Recursos	Inclusión en los proyectos de inversión actividades del MSPI de acuerdo al alcance establecido.	**3**	En el documento remitido de autodiagnóstico del MSPI en el control A.6.1.5, se indica se han asignado recursos para la gestión de proyectos; por verificaciones adicionales adelantadas por la OCI en el marco del seguimiento a los proyectos de inversión se evidencia que en el proyecto de inversión 7511 *"Fortalecimiento de la capacidad administrativa y tecnológica para la gestión institucional de Capital"* se han asignado recursos financieros y humanos para la implementación del MSPI en Capital, dando cumplimiento del requisito normativo.

7.4.2	Competencia, toma de conciencia y comunicación	Plan de cambio, cultura, apropiación, capacitación y sensibilización de seguridad y privacidad de la información (PIC).	**2**	El área de Sistemas indica que "Plan de cambio, cultura, apropiación, capacitación y sensibilización de seguridad y privacidad de la información (PIC)"; respecto al cual se adelanta la verificación de ejecución identificando que se adelantaron diversas actividades a lo largo de las vigencias 2022 - 2023, sin embargo, dicho plan no cuenta con herramientas que permitan efectuar seguimientos y monitoreos sobre su ejecución, de manera adicional se relacionan reportes adelantados al Plan de Acción Institucional, Plan de Fortalecimiento Institucional, identificación de riesgos de seguridad digital [sin relación de las actas de reunión indicadas], no se evidencia la implementación de las encuestas de satisfacción relacionadas, entre otros. Lo anterior, teniendo en cuenta que el documento fue elaborado durante la vigencia 2021 sin modificaciones en la vigencia 2022 y primer semestre de 2023. Teniendo en cuenta lo indicado, se recomienda al área articular la revisión anual del documento, de manera que se puedan identificar las actividades requeridas en materia de seguridad de la información con los colaboradores de Capital, las cuales pueden coordinarse con el área de Recursos Humanos e inclusión en el PIC en caso de requerirse la ejecución por parte de externos.
8.	**OPERACIÓN**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
8.1	Planificación e implementación	Plan de implementación de controles de seguridad y privacidad de información con: - Controles - Actividades - Fechas - Responsable de implementación y presupuesto.	**1**	Capital no cuenta con la definición de un plan de implementación de controles de seguridad y privacidad de la información que contemple los requisitos mínimos normativos, teniendo en cuenta que "El área de sistemas implementa los controles definidos en la ISO 27001: 1. Se cuenta con la matriz SoA, aplicabilidad de los controles de la ISO 27001. 2. Instrumento MSPI del MINTIC"; sin embargo, los documentos referenciados no cuentan con actividades, fechas, responsable de implementación y el presupuesto requerido. Teniendo en cuenta lo anterior, se recomienda al área adelantar el análisis de las herramientas para complementar lo requerido o definir una herramienta complementaria que permita controlar y monitorear la ejecución de los controles identificados, así como la efectividad de los mismos y definición de mejoras identificadas como parte del ciclo de vida del sistema.
9.	**Seguimiento, medición, análisis y evaluación**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
9.1.1	Seguimiento, medición, análisis y evaluación: Es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de éstos en el comité de gestión institucional y desempeño, como lo establece el MIPG.	*Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018. * Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.	**2**	En el plan de acción se encuentran incluidos los indicadores a través de los cuáles se mide el avance en el plan de implementación del plan de privacidad y seguridad de la información. A la fecha no se ha elaborado y socializado el informe de conformidad con el lineamiento que contenga la evolución y medición de la efectividad de los controles definidos en el plan de tratamiento de riesgos. Se indica por parte de los responsables que "en el plan de seguridad de la información se contempla el análisis del resultado obtenido con la evaluación del instrumento del MSPI", sin embargo, no se cuenta con un documento/informe con los resultados de acuerdo con el lineamiento normativo.
9.1.2	Auditoría Interna: Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.	*Resultados de las auditorías internas. *No conformidades de las auditorías internas. *Plan de auditorías que evidencia la programación de las auditorías de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de	**2**	Para la vigencia 2022 no se realizaron auditorías al MSPI. Para la vigencia 2023 se incluyó la auditoría dentro del Plan Anual de Auditoría [construido por la Oficina de Control Interno] el cuál fue aprobado por el CICCI y corresponde al presente informe.

		Coordinación de Control Interno.		
9.1.3	Revisión por la dirección: Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.	*Revisión a la implementación *Acta y documento de Revisión por la Dirección. *Compromisos de la Revisión por la Dirección.	**2**	La política de seguridad y privacidad de la información fue aprobada en el CIGD del 24/09/2020,sin embargo, no se cuentan con actas y/o soportes que permitan evidenciar la revisión periódica por la Alta dirección. El Manual de políticas complementarias de Seguridad de la Información así como el Manual del SGSI no fueron aprobados por la Alta dirección.
10.	**Mejoramiento Continuo**			
Numeral	**Lineamiento**	**Salida**	**Estado del requisito**	**Observaciones**
10.1	Mejora: Es importante que las entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.	Plan anual de mejora del MSPI	**1**	De conformidad con la respuesta de los responsables, no se ha formulado un plan de mejoramiento producto de los resultados del autodiagnóstico del MSPI, *"se realizan acciones en el plan de seguridad y privacidad de la información para su implementación, seguimiento y mejora continua de los dominios que presentan una calificación por debajo del nivel óptimo*". Es importante resaltar que si bien el ejercicio de autodiagnóstico del MSPI no genera hallazgos o incumplimientos, sí se evidencian debilidades en las etapas de levantamiento de información o de ejecución de controles sobre las cuáles y de conformidad con el presente requisito normativo es pertinente establecer un plan de mejora que permita evidenciar las acciones de mejora para que el Modelo llegue a un nivel de madurez optimizado. Así mismo, los resultados obtenidos en el autodiagnóstico indican un cumplimiento del MSPI del 85%, lo que indica que hay un 15% para establecer acciones de mejora, que se vean reflejadas en un plan anual de mejora. De igual manera, se debe establecer mejoras para las debilidades producto de la presente auditoría.

11.4. VERIFICACIÓN CUMPLIMIENTO DE CONTROLES ISO 27001:2013

Teniendo en cuenta el conocimiento técnico y especializado requerido para verificar la totalidad de controles de seguridad definidos en la NTC ISO 27001, se tomó una muestra de 60 de 114 controles de la norma cuyo nivel de cumplimiento podía ser evaluado por el equipo auditor, para los parámetros de calificación se empleó la misma escala de valoración indicada para evaluar el documento maestro del MSPI, los ítems que tengan calificación de 1 y 2 requerirán la formulación de acciones de mejora.

Adicionalmente, se evidencia que durante la vigencia 2022 se actualizó la norma ISO 27001 a su versión 2022, por lo tanto, se realizó la comparación del control bajo la norma actualizada versus la norma de 2013, sin la inclusión de controles nuevos que no hayan sido evaluados en el autodiagnóstico aplicado por Capital durante la vigencia 2022. A continuación, se describe es resultado para los controles verificados:

Tabla 2. Ejecución de controles ISO 27001

CAPITAL, SISTEMA DE COMUNICACIÓN PÚBLICA

OFICINA DE CONTROL INTERNO

PAPEL DE TRABAJO	
Auditoría:	Auditoría a las normas de Gestión: Sistemas de Gestión de Seguridad y Salud en el trabajo - SGSST y Norma ISO 27001: Seguridad de la Información.
Periodo evaluado:	1 de enero de 2022 al 31 de marzo de 2023.
IDENTIFICACIÓN DE LA ACTIVIDAD	
Tipo de evaluación:	Implementación de lineamientos y controles de la ISO 27001:2022
Auditor(es) responsable(s):	Jizeth González / Diana Romero

Fecha ejecución:	jun-23
Objetivo:	Verificar el nivel de implementación de los requerimientos de la ISO 27001:2022 [controles] en Capital.

5. Controles organizacionales					
Numeral ISO 27001/2022	**Numeral ISO 27001/2013**	**Control**	**Soporte**	**Operación del control**	**Observaciones**
5.1	A.5.1	Políticas de seguridad de la información	Política de seguridad de la información definida, aprobada, publicada, comunicada e interiorizada. Revisada a intervalos planificados.	**2**	La política se define en 2020 fue aprobada por el Comité Institucional de Gestión y Desempeño el 24 de septiembre; sin embargo, se evidencian debilidades respecto a la definición de los objetivos tanto general como específico, de igual manera, no se evidencia la documentación o registro de revisiones periódicas, se evidencia desactualización del marco legal, responsabilidades definidas que no atienden a los lineamientos de la política de administración de riesgos y a la realidad de la entidad teniendo en cuenta que el Comité Institucional de Gestión y Desempeño no actualiza y presenta la metodología para el análisis de riesgos, de conformidad con lo indicado en el artículo 5 de la Resolución 081 de 2021 es función del Comité aprobar la política y por ende hacerle seguimiento, así mismo teniendo en cuenta lo formulado en la Política de Administración del riesgo es responsabilidad de la segunda línea definir la metodología de administración del riesgo.
5.2	A.6.1.1	Roles y responsabilidades de seguridad de la información	Los roles y responsabilidades definidas y asignadas de acuerdo a las necesidades de la organización.	**2**	Los roles y responsabilidades definidos en la Política de seguridad y privacidad de la información tienen debilidades, teniendo en cuenta que no se evidencian responsabilidades en materia de ciberseguridad y T.I., de igual manera, estás no guardan coherencia con la política de administración del riesgo, las cuales se establecen en el numeral 6 de roles y responsabilidades de la Política de administración del riesgo aprobada el 5 de diciembre de 2022 por el Comité Institucional de Gestión y Desempeño.
5.3	A.6.1.2	Segregación de deberes	Separación de deberes conflictivos y áreas conflictivas.	**2**	Se establecen responsabilidades y deberes en la política de seguridad y privacidad de la información que permitan darle un uso adecuado a los activos; sin embargo, las responsabilidades identificadas en el numeral 7 de dicho documento para los actores: Gerencia, Comité Institucional de Gestión y Desempeño, y otros de segunda [Sistemas] y tercera línea de defensa [Oficina de control interno], no guardan coherencia con lo definido en el numeral 6 de roles y responsabilidades de la Política de administración del riesgo aprobada el 5 de diciembre de 2022 por el Comité Institucional de Gestión y Desempeño.
5.7	A.16.1.2	Inteligencia de amenazas	Información relacionada con las amenazas recopiladas y analizadas.	**1**	Si bien el área adelantó el uso del formato AGRI-SI-FT-040 Reportes de incidentes de seguridad en el que se registra el ataque a la intranet, no es posible observar la relación del documento de vulnerabilidad entregado por CSIRT Gobierno de Chile durante la vigencia 2022; así mismo, tampoco es posible evidenciar la trazabilidad de ejecución de las acciones formuladas, ni el impacto de estas en la documentación en materia de seguridad. Con base en lo anterior, se hace necesario que se documente la gestión de amenazas de manera clara [elaboración de informes que permitan tener una trazabilidad de las acciones adelantadas], y, de igual manera adoptar acciones de mejora, mitigando el impacto económico debido a gastos no planeados por ataques de seguridad.
5.8	A.6.1.5	Seguridad de la información en la gestión de proyectos.	La seguridad de la información se integrará a la gestión de proyectos.	**1**	Los responsables en el autodiagnóstico del MSPI indican que para dar cumplimiento a este requisito normativo se cuenta con *"la carpeta compartida contractual de la entidad"*, si bien, la inclusión de cláusulas en materia de seguridad de la información previene la materialización de riesgos en la ejecución contractual, el requisito normativo es mucho más amplio y solicita: "la seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza", lo que implica que para cada proyecto de la entidad (de inversión, misional, de las áreas de apoyo, creación de un nuevo ERP etc.) se deben identificar riesgos de seguridad de la información específicos para el proyecto, esta actividad no se realiza, cómo se ha indicado reiteradamente en los informe de gestión de riesgos realizados por la OCI: Capital no identifica riesgos específicos de seguridad de la información para los proyectos que gestiona.
5.9	A.8.1.1	Inventario de información y activos asociados.	Desarrollar y mantener un inventario de la información y activos asociados, incluyendo los responsables.	**2**	Se observa el inventario de activos de información publicado en la página web de Capital [https://www.canalcapital.gov.co/sites/default/files/activos-informacion/AGRI-SI-FT-038%20INVENTARIO%20Y%20CLASIFICACION%20DE%20ACTIVOS%20DE%20INFORMACION_CONSOLIDADO.xlsx]; sin identificación de vigencia, por lo

					que no es posible determinar la trazabilidad de actualización y modificación del documento. Así mismo, se evidencian debilidades de identificación de información en el marco de las TRD convalidadas de Capital, teniendo en cuenta el proceso de actualización de las TRD de Capital, sin que esto indique que se convalidarán por el Comité de Archivo.
5.10	A.8.1.3	Uso aceptable de la información y activos asociados.	* Identificación, documentación e implementación de reglas para uso aceptable. * Procedimiento para manejo de la información y activos asociados.	**2**	Capital cuenta con documentación de uso de la información y activos mediante el AGRI-SI-MN-006 Manual de políticas complementarias de seguridad de la información, AGRI-SI-PO-002 Política de seguridad y privacidad de la información, así como AGRI-SI-GU-001 Guía para el inventario y la clasificación de activos de información, dentro de estos se definen responsabilidades para uso de los activos de información para cada rol dentro del canal. Respecto a estos se debe complementar las políticas y responsabilidades frente a escenarios de acoso, difamación, suplantación de identidad, compras no autorizadas de manera articulada con la documentación existente en materia de contratación y de ingreso, mantenimiento y retiro de personal emitidos por el área de Talento Humano.
5.11	A.11.2.5	Devolución de activos	Los colaboradores devolverán todos los activos de la entidad que estén en su poder al cambiar o terminar contrato.	**1**	El área no cuenta con procedimientos definidos para la devolución de activos en el Manual de uso de recursos tecnológicos; sin embargo, al consultar sobre el control, se informó por parte del área de Sistemas que se cuenta con el formato [Google formularios] de control y salida de equipos, en el cual se lleva el control de devoluciones. Para las vigencias 2022 y corrido de 2023 se identificaron (62) elementos con salida (uno (1) sin aprobación de sistemas, de estos, 37 elementos no registran su devolución a la fecha, dentro de estos se evidenciaron dos (2) contratistas que no se encuentran vinculados a Capital. De conformidad con lo identificado, no es posible determinar que el control que se adelanta sea efectivo para mitigar la pérdida de elementos al interior de Capital. Para lo anterior, se hace necesario que se documente el proceso o procedimiento correspondiente que permita determinar las actividades requeridas para controlar el trámite adelantado respecto a la salida e ingreso de elementos prestados para uso por parte de los colaboradores de Capital y otros como revisión y reparación y a su vez se realice una articulación con las demás áreas (Servicios Administrativos y Área Técnica) que tienen a su cargo la administración de activos de Capital.
5.12	A.8.2.1	Clasificación de la información	Clasificar la información en función de confidencialidad, integridad, disponibilidad y requisitos pertinentes.	**2**	Se observa el inventario de activos de información publicado en la página web de Capital [https://www.canalcapital.gov.co/sites/default/files/activos-informacion/AGRI-SI-FT-038%20INVENTARIO%20Y%20CLASIFICACION%20DE%20ACTIVOS%20DE%20INFORMACION_CONSOLIDADO.xlsx]; sin identificación de vigencia, por lo que no es posible determinar la trazabilidad de actualización y modificación del documento. Así mismo, se evidencian debilidades de identificación de información en el marco de las TRD convalidadas de Capital. De igual manera, se observa que se vienen adelantando actualizaciones del documento teniendo en cuenta el proceso de actualización de las TRD de Capital [sin que estas se encuentren convalidadas por el Comité Distrital de Archivo]
5.13	A.8.2.2	Etiquetado de información	Procedimiento para el etiquetado de la información de conformidad con la clasificación de la información adoptado.	**3**	Capital cuenta con documentación de lineamientos para el etiquetado de información en el marco de la gestión del repositorio digital como es AGRI-GD-GU-002 Guía de lineamientos para el uso y almacenamiento de documentos digitales y/o electrónicos en canal capital, de manera que los expedientes conserven los principios de orden original, en coherencia con las Tablas de retención Documental (TRD) y cuadros de clasificación de activos de información. Se recomienda tener en cuenta la revisión, actualización y socialización que deberá realizarse en el marco de la actualización de TRD de Capital y demás documentos con la implementación en proceso del ERP que se viene construyendo en Capital.
5.14	A.13.2	Transferencia de información	Reglas, procedimientos y acuerdos de transferencia de información dentro de la organización y entre la organización y otras partes.	**2**	Se cuenta con los procedimientos de transferencias primarias [AGRI-GD-PD-001] y secundarias [AGRI-GD-PD-002] para Capital, documentados por el área de Gestión Documental, en los que se establecen los lineamientos requeridos para transferencia; sin embargo, estos no contemplan la información digital emitida por las áreas a la fecha de la presente evaluación, así como los lineamientos determinados en la Política de gestión Documental y el Manual de Gestión Documental.
5.15	A.9.2.2 A.9.2.3	Control de acceso	Reglas para controlar el acceso físico y lógico de la información y otros activos asociados en función de requisitos de seguridad y privacidad de la información.	**1**	Se informa por parte del área que se cuenta con el documento AGRI-GD-IN-002 Instructivo Tablas de control de acceso de la vigencia 2022 en el que se identifican los lineamientos y tablas de control de acceso; sin embargo, las TRD se encuentran en proceso de modificación y aprobación, así como convalidación por parte del Archivo Distrital. De igual manera, se cuenta con la publicación del AGRI-SI-MN-005 Manual de Gestión de Usuarios en su versión 02 del 13 de diciembre de 2021 en los que

					se detalla el paso a paso para activación y desactivación de usuarios y entrega de la información sensible como contraseñas y usuarios; sin embargo, adelantadas las pruebas se observó el incumplimiento de aspectos como: no se cuenta con Check List de instalación de software básico de conformidad con lo indicado en el numeral 4.1.7, así como el incumplimiento de lo determinado en el numeral 5 del procedimiento general de gestión de usuarios, al recibir solicitud de asociación de cuentas por parte de los trabajadores de Capital, no de parte del Supervisor de Contrato, Jefe Directo o Área de Recursos Humanos a otros usuarios por cubrimiento de vacaciones, así como tampoco se cuenta con soportes de respuesta aplicación del control respecto a la desactivación de las cuentas por vacaciones, incapacidad, retiro y demás motivos mencionados, ni soportes de activación al reingreso de los colaboradores de Capital. Respecto a la solicitud de información sobre desactivación por incapacidades se indicó por parte del área de sistemas que no se tuvo conocimiento de dichos eventos, por lo que se recomienda se adelante la debida actualización de las actividades descritas en el documento, así como la socialización a los líderes de área, jefes directos y colaboradores del área de recursos humanos, de manera que la información sea interiorizada y se dé cabal cumplimiento a lo formulado en los controles en materia de seguridad de la información.
5.16	A.6.1.5	Gestión de identidad	Gestión del ciclo de vida de la entidad.	**2**	El área de Sistemas indica que el ciclo de vida de la organización se encuentra reflejado en los avances de cumplimiento del ITIL; sin embargo, en las carpetas establecidas de estrategia, diseño, transición, operación, gestión de proyectos no se cuenta con información que permita evidenciar la aplicación de este control. La información suministrada dentro de la carpeta refiere la transición a IPV6, telefonía IP. Lo anterior, no puede relacionarse con el ciclo determinado de la ISO 27001 en lo referente al PHVA, en articulación con los documentos externos al área que guardan relación con la implementación del sistema; ejemplo, incluir en la caracterización del proceso o documentos pertinentes el ciclo mediante el cual Capital da cumplimiento a los requisitos normativos de la norma citada, de manera que se pueda identificar de manera clara el ciclo mediante el cual opera.
5.17	A.9.2.4	Información de autenticación	Asignación y gestión de la información de autenticación controlada mediante un proceso de gestión.	**2**	La asignación y gestión de la información de autenticación se adelanta mediante el formato de solicitud de servicios TIC [AGRI-SI-FT-029] el cual se gestiona vía Google Forms; sin embargo, para las vigencias 2022 - 2023 se identifica la solicitud de (56) activaciones de usuario nuevos, de las cuales se remite soportes de (11) actas de entrega de servicios TIC [AGRI-SI-FT-019] y en estas, cinco (5) cuentan con las firmas respectivas, por lo que no es posible establecer la efectividad del control identificado. De conformidad con lo indicado, se recomienda al área verificar las condiciones de suscripción de dicha acta, así como socialización de los parámetros identificados en el manual de gestión de recursos tecnológicos creado por el área de Sistemas.
5.18	A.9.2.3 A.9.2.6	Derechos de acceso	Proporcionar, revisar, modificar y eliminar los derechos de acceso de la información de acuerdo con la política.	**1**	Se adelanta prueba del control el 16 de agosto de 2023 en el que se indica por parte del área que se genera un informe mensual de depuración de cuentas del directorio activo de Capital, sin embargo, no se remite dicho informe consolidado. Con lo anterior, no es posible verificar que la depuración indicada se lleve a cabo y por ende, que el control sobre derechos de acceso sea efectivo respecto a lo requerido en materia de revisión, modificación y eliminación de conformidad con lo definido en la política de seguridad de la información y documentos articulados como el manual de gestión de usuarios. Si bien se remitieron pantallazos de eventos de privacidad del directorio activo, no cuenta con la relación de las actividades adelantadas en materia de depuración de usuarios no vinculados al canal.
5.19	A.15.1	Seguridad de la información en las relaciones con los proveedores.	Definir e implementar procesos y procedimientos para gestionar riesgos de seguridad de la información asociado a productos y servicios de los proveedores.	**2**	Desde el área jurídica se viene adelantando la identificación de riesgos por tipología de contratación, así mismo, desde Sistemas se adelanta la identificación de riesgos de seguridad digital y a nivel institucional se cuenta con la definición de política de administración del riesgo y manual de administración del riesgo; sin embargo, se requiere su revisión y ajuste de conformidad con el requerimiento del control, ya que en estos no se incluyen riesgos en materia de seguridad de la información asociado a productos y servicios de los proveedores, en función de los proveedores y asociados a la cadena de suministro de productos TIC, ya que se enfocan en el incumplimiento contractual, de contagio por COVID-19 y demoras en entrega de compras adelantadas. Para lo anterior, se requieren mesas de trabajo entre el área de sistemas, área técnica y de la oficina jurídica con el fin de que los riesgos

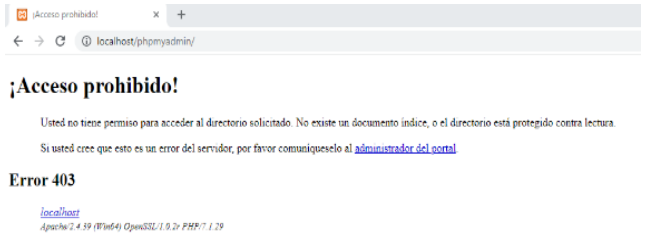
					cuenten con las características requeridas, herramienta de monitoreo y control, para medir la efectividad del control identificado.
5.20	A.15.2	Abordar la seguridad de la información en los acuerdos con los proveedores	Los requisitos de seguridad de la información se establecerán con el proveedor en función del proveedor.	**2**	Desde el área jurídica se viene adelantando la identificación de riesgos por tipología de contratación, así mismo, desde Sistemas se adelanta la identificación de riesgos de seguridad digital y a nivel institucional se cuenta con la definición de política de administración del riesgo y manual de administración del riesgo; sin embargo, se requiere su revisión y ajuste de conformidad con el requerimiento del control, ya que en estos no se incluyen riesgos en materia de seguridad de la información asociado a productos y servicios de los proveedores, en función de los proveedores y asociados a la cadena de suministro de productos TIC, ya que se enfocan en el incumplimiento contractual, de contagio por COVID-19 y demoras en entrega de compras adelantadas. Para lo anterior, se requieren mesas de trabajo entre el área de sistemas, área técnica y de la oficina jurídica con el fin de que los riesgos cuenten con las características requeridas, herramienta de monitoreo y control, para medir la efectividad del control identificado.
5.21	A.15.1 A.15.2	Gestión de la seguridad de la información en la cadena de suministro de TIC.	Definir e implementar procesos y procedimientos para gestión de riesgos asociados a la cadena de suministro de productos TIC.	**2**	Desde el área jurídica se viene adelantando la identificación de riesgos por tipología de contratación, así mismo, desde Sistemas se adelanta la identificación de riesgos de seguridad digital y a nivel institucional se cuenta con la definición de política de administración del riesgo y manual de administración del riesgo; sin embargo, se requiere su revisión y ajuste de conformidad con el requerimiento del control, ya que en estos no se incluyen riesgos en materia de seguridad de la información asociado a productos y servicios de los proveedores, en función de los proveedores y asociados a la cadena de suministro de productos TIC, ya que se enfocan en el incumplimiento contractual, de contagio por COVID-19 y demoras en entrega de compras adelantadas. Para lo anterior, se requieren mesas de trabajo entre el área de sistemas, área técnica y de la oficina jurídica con el fin de que los riesgos cuenten con las características requeridas, herramienta de monitoreo y control, para medir la efectividad del control identificado.
5.23		Seguridad de la información para el uso de servicios en la nube.	Procesos de adquisición, uso, gestión y salida de servicios en la nube establecidos en los requisitos de seguridad de la información.		En la mesa de aclaración de inquietudes sobre el informe preliminar de auditoría [realizada el 24 de octubre], se indica por parte del Jefe del área de Sistema que Capital sólo tiene un servicio en la nube el cual es la página web la cual esta alojada en Amazon. Al haber al menos un servicio se debe aplicar este control al servicio en la Nube. Este control no fue calificado con un nivel de implementación en el informe preliminar de auditoría puesto que **No se deberá adelantar plan de mejoramiento para este control durante la presente vigencia,** ya que el control 5.23 fue incluido en la versión de 2022 de la norma ISO 27001 la cual se usó como referente comparativo, para ir articulando el seguimiento de la próxima vigencia.
5.24	A.16.1.1	Planificación y preparación de la gestión de incidentes de seguridad de la información.	Planificar y preparar la gestión de información de gestión de incidentes, estableciendo roles y responsabilidades.	**2**	Capital cuenta con la guía de reporte de incidentes de seguridad [AGRI-SI-GU-007], así como los formatos de reporte de incidentes de seguridad; sin embargo, en el marco de la auditoría adelantada en la vigencia 2022 en materia de ISO 27001, se deben adelantar ajustes a la documentación diseñada de manera que sea acorde con los requerimientos del modelo de seguridad y privacidad de la información. Dentro de estas se identifica que el documento de Capital no registra la clasificación del incidente, tratamiento de incidentes por clasificación, cierre del incidente, gestión del conocimiento [registro de capacitaciones y socializaciones requeridas], así como el ajuste de las responsabilidades en el marco de la política de administración del riesgo y recomendaciones relacionadas en materia de identificación del riesgo.
5.25	A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	La organización evalúa los eventos de seguridad de la información y decidir si clasifican como incidentes.	**1**	Capital emite el documento AGRI-SI-GU-007 Guía de reporte de incidentes de seguridad; sin embargo, en este no se identifican los procesos de evaluación y decisión sobre los eventos de seguridad y si estos son clasificados como incidentes. Lo anterior, en coherencia del control A.16.1.1
5.26	A.16.1.5	Respuesta a incidentes de seguridad de la información	Responder a los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.	**1**	Si bien Capital cuenta con la AGRI-SI-GU-007 Guía de reporte de incidentes de seguridad y se adelantó el registro de las acciones a realizar en el formato AGRI-SI-FT-040 reportes de incidentes de seguridad; sin embargo, no se cuenta con soportes de la gestión adelantada, análisis de causas y cierre de la misma.

5.27	A.16.1.6	Aprender de los incidentes de seguridad de la información	Fortalecimiento y mejora de los controles de seguridad con el conocimiento obtenido.	**1**	No se evidencia registro, documentación o recolección de las lecciones aprendidas de los incidentes de seguridad, dentro de los cuales se considere el volumen de incidentes, la tipología de incidentes, de conformidad con la guía de reporte de incidentes, al igual que los costos, impactos y la solución de los incidentes registrados.
5.28	A.16.1.7	Recolección de evidencia	Establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia de incidentes.	**1**	Capital en el marco de la AGRI-SI-GU-007 Guía de reporte de incidentes de seguridad, diligencia el formato AGRI-SI-FT-040 reportes de incidentes de seguridad. con el cual se reúne información y se preserva, de conformidad con lo requerido en la norma. Sin embargo, no se observa el repositorio de evidencias en materia de identificación, tratamiento y cierre de incidentes.
5.30	A.17.1 A.17.2 A.17.3	Preparación de las TIC para la continuidad del negocio	Planificación, implementación, mantenimiento y prueba de las TIC para continuidad del negocio.	**1**	Si bien el área cuenta con un documento de continuidad del negocio, este no registra los elementos requeridos en materia de contexto de la organización, objetivos de continuidad del negocio, evaluación del impacto de negocio, evaluación de riesgos, estrategias y soluciones de continuidad del negocio, planes de continuidad del negocio, de conformidad con lo definido en la ISO 22301:2019. Por lo anterior, se hace necesario realizar la verificación y actualización del plan de continuidad vigente, teniendo en cuenta los requerimientos de la ISO 23301:2019; por lo que es importante que se adelante la estructuración de un documento que cuente con: un alcance, referencias normativas aplicables, términos y condiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. De igual manera, se adelantaron pruebas en materia de existencia de equipos relacionados en el documento de continuidad vigente, observando que no se realiza el uso de aplicativos relacionados, así como la falta inclusión de nuevos elementos como los módulos del ERP y actualizaciones no relacionadas.
5.31	A.18.1.1	Requisitos legales, estatutarios, reglamentarios y contractuales	Identificarse, documentarse y mantenerse los requisitos legales, estatutarios, reglamentarios y contractuales.	**2**	Capital cuenta con el normograma, publicado en la intranet [https://intranet.canalcapital.gov.co/intranet/docdowncc/DocSistema/2023/Norma/Normograma%20Institucional%20Canal%20Capital%20(2023.01.06).xlsx] en el cual se registran las normas aplicables al proceso, si bien no se evidencia la fecha de actualización, es importante que se adelante la inclusión de normatividad en materia de gobierno digital, seguridad de la información, entre otros.
5.36	A.5.1 A.5.2	Cumplimiento de políticas, normas y estándares de seguridad de la información	Cumplimiento de la Política de seguridad y privacidad de la información, comunicación, revisión periódica.	**1**	La AGRI-SI-PO-002 Política de seguridad y privacidad de la información no contempla acciones de monitoreo o evaluación del cumplimiento de las acciones que permita evidenciar de manera clara el cumplimiento de las actividades formuladas en materia de seguridad y privacidad de la información. No hay soporte que permita evidenciar la revisión periódica por la Alta Dirección.

6. Controles de personas

Numeral ISO 27001/2022	Numeral ISO 27001/2013	Control	Soporte	Operación del control	Observaciones
6.1	A.7.1.1	Poner en pantalla	Verificación de antecedentes de los colaboradores previo a unirse a la organización, teniendo en cuenta la clasificación de la información a la que accederá.	**3**	Se tomó una muestra de seis (6) contratos de los contratistas vinculados al área de Sistemas correspondientes a las vigencias 2022 y 2023, dentro de los cuales se observa la consulta adelantada ante la Procuraduría, Contraloría, Personería, Policía y de Medidas Correctivas. De manera adicional para los ingenieros se cuenta con la consulta al COPNIA respectivamente.
6.2	A.7.1.2	Términos y condiciones de empleo	Los acuerdos contractuales deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.	**2**	Se realizó la verificación de (39) expedientes correspondientes a colaboradores de todas las áreas de Capital respecto a los acuerdos contractuales en los que se establecen responsabilidades en materia de seguridad de la información, sobre lo cual se identificó que en la totalidad se establece una cláusula con seis (6) requisitos a cumplir por parte del contratista; sin embargo, no se evidencian las responsabilidades de la entidad en materia de seguridad de la información, así como tampoco se identifican documentos que contengan este tipo de responsabilidades establecidas, comunicadas y/o socializadas al colaborador a vincular en la organización.
6.3	A.7.2.2	Concientización, educación y capacitación en seguridad de la información.	El personal debe recibir educación y capacitación adecuadas en seguridad de la información y actualizaciones de la	**1**	Capital cuenta con el Plan AGRI-SI-PL-005 PLAN DE SENSIBILIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN de la vigencia 2021 en su versión 1; sin embargo, consultando los soporte al área responsable se indica que "... es de aclarar que este plan se encuentra en proceso de actualización, está en proceso de revisión por parte de Planeación"

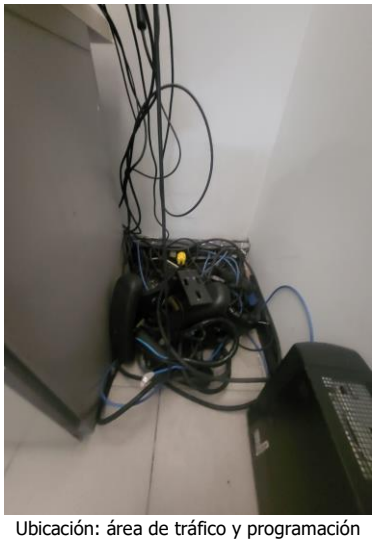
			política de seguridad de la información, políticas y procedimientos específicos del tema.		por lo que a la fecha no se adelantan capacitaciones, socializaciones u otras en materia de seguridad de la información.
6.5	A.7.3.1	Responsabilidades después de la terminación o cambio de empleo	Definición, aplicación y comunicación al personal las responsabilidades y deberes de seguridad de la información que sean válidos después de terminación o cambio de empleo.	**2**	Si bien se definen en las cláusulas contractuales de los colaboradores de Capital el requisito de *"Una vez ejecutado el contrato en su totalidad, el CONTRATISTA se obliga a devolver de inmediato al supervisor del contrato, toda la información y documentos y/o materiales entregados, o a los que llegare a tener conocimiento, por cualquier motivo, contenidos en cualquier medio, y toda copia de ella, facilitados para el desarrollo de la labor contratada. Igualmente, por solicitud de CANAL CAPITAL, deberán proceder a la destrucción de la información confidencial y documentos y/o materiales entregados, así como certificar ello por escrito, en cada relación individualmente consideradas"*, sobre lo cual no se observa en la terminación de contratos esta comunicación y certificación; así mismo, respecto a la aplicación se establecen los lineamientos en el Manual de supervisión e interventoría [AGJC-CN-MN-002]. Por lo que se recomienda la coordinación de jornadas entre las áreas de Sistemas y de la Oficina Jurídica, de manera que dichas cláusulas y requerimientos sean comunicadas e interiorizadas las responsabilidades y deberes de ambas partes en materia de seguridad de la información válidas después de la terminación o cambio de empleo.
6.6	A.7.3.1	Acuerdos de confidencialidad o no divulgación	Identificar, documentar y revisar regularmente los acuerdos de confidencialidad o no divulgación para la protección de la información.	**2**	El área de Recursos Humanos cuenta con el formato AGTH-FT-083 Acuerdo de confidencialidad y no divulgación para los funcionarios de planta. Sin embargo, para los contratistas no hay un formato para la suscripción de acuerdos prestación de servicios, teniendo en cuenta que si bien la minuta de contratos cuenta con la definición de una cláusula con seis (6) requisitos en materia de responsabilidad del contratista respecto a la seguridad de la información; sin embargo, este no cuenta con la definición de las obligaciones por parte de Capital. Por otro lado, como se indica en el numeral anterior, se define el requisito de "Una vez ejecutado el contrato en su totalidad, el CONTRATISTA se obliga a devolver de inmediato al supervisor del contrato, toda la información y documentos y/o materiales entregados, o a los que llegare a tener conocimiento, por cualquier motivo, contenidos en cualquier medio, y toda copia de ella, facilitados para el desarrollo de la labor contratada. Igualmente, por solicitud de CANAL CAPITAL, deberán proceder a la destrucción de la información confidencial y documentos y/o materiales entregados, así como certificar ello por escrito, en cada relación individualmente consideradas", sobre lo cual no se observa comunicación o el certificado indicado; así mismo, respecto a la aplicación se establecen los lineamientos en el Manual de supervisión e interventoría [AGJC-CN-MN-002]. Por lo que se recomienda la coordinación de jornadas entre las áreas de Sistemas y de la Oficina Jurídica, de manera que dichas cláusulas y requerimientos sean comunicadas e interiorizadas al igual que las responsabilidades y deberes de ambas partes en materia de seguridad de la información.
6.7	A.6.2.2	Trabajo remoto	Implementación de políticas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones.	**2**	Desde el área de Recursos Humanos se publicó la Resolución 118 de 2023 mediante la cual se regula el teletrabajo, y desde el área de Sistemas se establecen políticas de conexión a los servidores garantizando la seguridad del equipo. Sin embargo, en la prueba adelantada el 16 de agosto de 2023, se indicó por parte del área de Sistemas que el alcance del trabajo adelantado no puede amparar la información que se maneja en equipos personales o que son extraídos en el marco de la ejecución de las obligaciones laborales. Por lo anterior, se adelanta la recomendación de verificar medidas que puedan ser implementadas, socializadas e interiorizadas en materia de seguridad de la información a la que se accede, procesa y almacena fuera de las instalaciones de Capital.
6.8	A.16	Informes de eventos de seguridad de la información	Proporcionar mecanismos para que el personal informe de eventos de seguridad de la información de manera oportuna.	**2**	Se indica por parte del área que dentro de los mecanismos para informar eventos de seguridad de la información se cuenta con el correo electrónico, en el cual el colaborador puede comunicar los eventos de seguridad, una vez reportado, el área de Sistemas adelanta el reporte en el formato AGRI-SI-FT-040, con el resumen de lo sucedido, fecha, análisis y actividades ejecutadas; sin embargo, estos no son mencionados en la AGRI-SI-GU-007 GUIA DE REPORTE DE INCIDENTES DE SEGURIDAD, versión 2 del 13 de diciembre de 2021. Para la vigencia 2022 se presentó un (1) incidente de seguridad: Anomalía o vulnerabilidad de software [15 de marzo de 2022], sobre el cual se determinaron acciones para atención del impacto; sin embargo, teniendo en cuenta la información suministrada durante la prueba no se registra la totalidad de actividades realizadas en equipos de la entidad y demás equipos

					tecnológicos de los colaboradores afectados para análisis de mejoras a implementar.  **Fuente:** Reporte incidentes - Sistemas

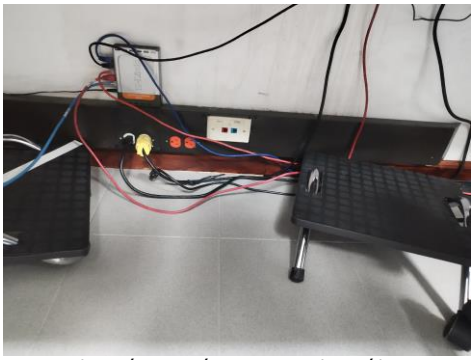
7. Controles físicos					
Numeral ISO 27001/2022	**Numeral ISO 27001/2013**	**Control**	**Soporte**	**Operación del control**	**Observaciones**
7.1	A.11.1.1	Perímetros físicos de seguridad	Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.	**2**	Capital ha definido controles de acceso para el ingreso de colaboradores y externos a las Sedes. Se tiene un área de recepción con vigilancia para controlar el acceso físico a las sedes; el acceso está restringido únicamente para personal autorizado. Al Datacenter sólo tienen acceso el personal del área de Sistemas, mediante huella digital y cualquier ingreso será aprobado por los mismos, se lleva un registro del ingreso de personas al datacenter. De conformidad con las pruebas definidas en la matriz de autodiagnóstico del MSPI, se debe fortalecer el numeral f) instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; "***las áreas no ocupadas deben tener alarmas en todo momento***"**;** también deben abarcar otras áreas, tales como las salas de cómputo o las salas de comunicaciones. (Negrilla fuera de texto). Se evidenciaron botones de emergencia en varios espacios de la sede de la calle 26, sin embargo, ni los colaboradores del área de Sistemas, ni de Servicios Administrativos tienen conocimiento de la función de los botones, qué acciones suceden si se activan, por lo cual, no se tiene conocimiento de si las alarmas instaladas en la Sede de la calle 26 son funcionales, en la Sede de la Calle 69 no se cuentan con alarmas para activar en caso de detección de intrusos.  **Fuente:** Área Sistemas - Salida.

					 **Fuente:** Área Sistemas - Data Center (Calle 26). Así mismo, se observa que las puertas de la sede de la Calle 26 permanecen abiertas; y, dado que la pandemia causada por COVID-19 finalizó el 30 de junio de 2022 [Resolución 666 de 2022] se recomienda reactivar el ingreso con las tarjetas de control con las que cuenta el Canal, de manera que se mitiguen accesos indebidos y se mantenga la seguridad perimetral de Capital.
7.5	A.11.2.1	Protección contra amenazas físicas y ambientales.	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura	**2**	De conformidad con el control A.11.2.4 de la ISO 27001:2013, se deben diseñar e implementar controles contra amenazas físicas y ambientales, en la matriz de riesgo se encuentran identificadas amenazas físicas, sin embargo, amenazas de tipo ambiental como fenómenos climáticos, físicos, inundación, sísmicos, meteorológicos no se han documentado, ni formulado controles para minimizar el riesgo de afectaciones en la privacidad y seguridad de la información. Lo anterior, como se indica en el numeral 11.7. del presente informe.
7.7	A.11.2.9	Escritorio despejado y pantalla despejada	Se deben definir y hacer cumplir apropiadamente reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y reglas de pantalla limpia para instalaciones de procesamiento de información.	**2**	En el manual de políticas complementarias se establecen las políticas de escritorio y pantalla limpia, de conformidad con el requisito normativo; sin embargo, falta incluir dentro del manual: Establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada. Lo anterior, es indispensable en las áreas dónde no se cuentan con puertas de seguridad como la mayoría de espacios de la Sede Quinta Camacho y el área de la Calle 26 dónde realizan sus labores las áreas misionales. Adicionalmente, se establece en el Manual que ***"No se debe ingerir bebidas o comida en los puestos de trabajo"***, política que no es conocida por los colaboradores consultados durante las pruebas de recorrido por lo cual en varios puestos de trabajo se puede observar el consumo de alimentos y bebidas, adicionalmente, no se encuentra esta prohibición en avisos, carteleras, afiches etc. para instruir a los colaboradores, por lo anterior, es pertinente revisar la prohibición, informando adicionalmente los espacios donde sí se pueden consumir alimentos, sumado a lo mencionado, es importante revisar la capacidad de los espacios aprobados para el consumo de estos en cada una de las Sedes de Capital [Calle 69 - Calle 26], con el fin de evitar que se adelante el consumo de alimentos en el puesto de trabajo.
7.8	A.11.2.8	Emplazamiento y protección de equipos	El equipo se colocará en forma segura y protegida	**2**	Para los equipos de Capital se puede evidenciar que: Se incluyó en el Manual de políticas complementarias que los funcionarios, proveedores, socios de negocio y terceros que tengan a cargo estaciones de trabajo o equipos tecnológicos de propiedad de Canal Capital deben bloquear estos en el momento de abandonar el puesto de trabajo con el fin de proteger el acceso indebido a la información en estos almacenada. Sin embargo, no se establece en el Manual de políticas complementarias que los equipos de usuarios desatendidos se aseguraran mediante un mecanismo

					de bloqueo apropiado (un protector de pantalla protegido con contraseña). No existe un parámetro de tiempo estándar para que los equipos de Capital se bloqueen automáticamente de forma segura, en las pruebas realizadas se evidenció que hay equipos que se bloquean al minuto y otros casos donde el bloqueo se da a los diez minutos, lo que expone la privacidad y seguridad de la información, ya que, que si el colaborador deja de usar su equipo y se retira de las instalaciones sin bloquear, este puede tardar hasta diez minutos antes de bloquearse automáticamente. Teniendo en cuenta lo indicado, se recomienda fortalecer los lineamientos estructurados mediante el establecimiento de los mecanismos de bloqueo seguro, así como la ejecución de campañas de sensibilización y socialización respecto a dichos lineamientos en materia de protección de la información.
7.9	A.11.2.6	Seguridad de los activos fuera de las instalaciones	Se protegerán los activos fuera del sitio.	**2**	En el manual de políticas complementarias se establecen lineamientos para el teletrabajo, así mismo los activos de Capital se encuentran asegurados en caso de pérdida, daño o hurto, y cuentan con software licenciado y antivirus. De conformidad con las pruebas definidas en la matriz de autodiagnóstico del MSPI, se deben fortalecer el manual de políticas complementarias definiendo lineamientos que orienten a los colaboradores a ejecutar los siguientes criterios de seguridad de los activos fuera de las instalaciones, de conformidad con el requisito normativo: a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos; b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes); c) controlar los lugares fuera de las instalaciones, tales como trabajo en casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina); d) establecer que cuando el equipo que se encuentra fuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo [Para lo cual se deben tener en cuenta los lineamientos definidos en la guía de evidencia digital - Seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia].
7.11	A.11.2.2	Utilidades de apoyo	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.	**3**	El data center ubicado en la Sede de la Calle 26 cuenta con un respaldo ante cortes de energía de una UPS de 80KVA, adicionalmente el edificio cuenta con un sistema autónomo de generación de energía de 500 KVA, la Sede de la Casa de la 69 cuenta con un respaldo ante cortes de energía de una UPS de 40KVA que permite tomar acciones de respaldo al momento de cortes de luz. Sin embargo, se recomienda al área adelantar la verificación y actualización del plan de continuidad vigente, teniendo en cuenta los requerimientos de la ISO 23301:2019; por lo que es importante que se adelante la estructuración de un documento que cuente con: un alcance, referencias normativas aplicables, términos y condiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora. Incluyendo los elementos correspondientes [los cuales se pueden inventariar de manera externa] que permita mantener actualizado el documento y sus anexos a la necesidad de Capital.
7.12	A.11.2.3	Seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.	**2**	De conformidad con lo indicado por los responsables todo el cableado horizontal se encuentra en canaletas metálicas para protegerlos de intercepciones, interferencias o daños. En la sede de la Casa de la 69, se puede evidenciar que todo el cableado está de conformidad con lo indicado, sin embargo, en la Sede de la calle 26 se evidencian cables que transportan energía, datos o servicios de información expuestos a daños, como se evidencia en las siguientes imágenes:



Ubicación: área de tráfico y programación



Ubicación: Gestión Documental - Jurídica

8. Controles Tecnológicos					
Numeral ISO 27001/2022	**Numeral ISO 27001/2013**	**Control**	**Soporte**	**Operación del control**	**Observaciones**
8.2	A.9.2.3	Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará	**1**	Si bien en el Manual de Políticas Complementarias de seguridad de la información en el numeral 5.4 se establece la Política de control de acceso, esta se establece como una necesidad *"de que Capital debe implementar controles"* más no cumple con las características de una política de conformidad con el Manual para el control de documentos institucionales, versión 5: *Política: Documento que contiene los criterios o directrices de acción elegidos como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos del nivel institucional.* Lo anterior, teniendo en cuenta lo definido en la NTC ISO 27001 2013 que señala lo siguiente: *"Se debe establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso"*, es necesario que la política cumpla con las características que debe tener este lineamiento.
8.3	A.9.1.1	Restricción de acceso a la información	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.	**1**	Teniendo en cuenta lo indicado en el control A.9.2.3, se deben adelantar las acciones correspondientes para la documentación de la política requerida. Así mismo, en el Manual de Políticas Complementarias, en el que se encuentra definido el numeral 5.4. Política de Control de Acceso, se define la restricción al acceso de información y se indican las responsabilidades de todos los niveles de la organización; sin embargo, falta complementar la responsabilidad del área de Recursos Humanos frente a las novedades de retiro, vacaciones o incapacidades en los siguientes numerales, ya que, no está estipulada la responsabilidad del área: - Numeral 5.2.2 Durante la Ejecución del Empleo: El área de RH debe notificar al área de Sistemas los periodos de vacaciones, licencias y/o incapacidades de funcionarios de planta para desactivar los servicios y acceso a la información durante la ausencia del funcionario, y en el caso del correo electrónico redireccionarlo a la cuenta autorizada. - Numeral 5.2.3 Terminación y Cambio de Empleo: El área de RH debe notificar al área de Sistemas de la terminación del contrato de un funcionario de planta, ya que no hay una inactivación automática de los servicios como en caso de los contratistas que tienen una fecha de terminación estipulada.
8.5	A.9.1.2 A.9.2.3 A.9.2.4	Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso	**1**	Los funcionarios y usuarios de Capital deben autenticarse para hacer uso de: -El ingreso a las instalaciones físicas del canal (Carnet institucional, tarjeta de acceso), si es invitado debe portar escarapela, esta escarapela aplica para la sede de la Calle 26, para la sede de la Casa de 69 no se han definido lineamientos para la identificación de terceros. -El uso de las redes de internet -El uso de los computadores -Acceso a la intranet y ERPs -Acceso a las carpetas de información de conformidad con las TRD Sin embargo, teniendo en cuenta lo indicado en el control A.9.2.3, se deben adelantar las acciones correspondientes para la documentación de la política requerida.
8.6	A.12.1.3	Gestión de Capacidad	El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y esperados. Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	**1**	Para medir la gestión de la Capacidad el área de Sistemas diligencia la Matriz CMDB de inventarios de Canal, con respecto a esta matriz se evidencian pestañas con información incompleta, ya que, faltan varias columnas con información sobre los equipos por diligenciar: -Pestaña Scanner -Pestaña Servidores -Pestaña CI-LAN,WLAN, WAN -Pestaña UPS -Pestaña Videobeam -Pestaña Impresoras -Pestaña Aplicaciones Al encontrarse incompleta esta información no es posible determinar, el estado actual de la gestión de la Capacidad de Capital. En cuanto a los requisitos de capacidad esperada se indica que se encuentran señalados en la Hoja de Ruta del PETI, para le PETI deben atenderse las recomendaciones indicadas en el numeral 11.5

8.8	A.12.6	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.	**2**	Se realizó un informe de vulnerabilidades técnicas en noviembre de 2022, en este se identificó la vulnerabilidad que tiene Capital en cuanto a: - El sitio www.canalcapital.gov.co presenta vulnerabilidades de riesgo alto en la url. De conformidad con los lineamientos del MSPI, para las vulnerabilidades identificadas se deberá: Establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado, frente a lo anterior, no se evidencia documento en el cual se haya realizado el respectivo análisis de riesgos, ni las gestiones adelantadas para mitigar el riesgo detectado.
8.10	A.11.2.7	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria	**2**	Capital cuenta con Guía de Borrado Seguro de Información V2, donde se definen los lineamientos adoptados por la entidad para borrar de forma segura la información, indicando los diferentes métodos que existen y sus ventajas y desventajas, sin embargo, se recomienda definir en la guía quién ejercerá la responsabilidad final de verificar que la información se haya eliminado segura y definitivamente, ya que no se establece ese punto de control. Se indica por los responsables que se encuentra en proceso de construcción la guía de alistamiento de equipos de cómputo, que se complementará para este tema, Lo anterior, se detalla en el numeral 11.5. del presente informe.
8.11	A.9.4.5	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.	**1**	De conformidad con lo indicado por los responsables no se cuenta con políticas o lineamientos específicos para el enmascaramientos de datos.
8.13	A.12.3.1	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada	**1**	No se cuenta con una política de copias de seguridad, se cuenta con un procedimiento, sin embargo, en las políticas de operación del procedimiento no se define la realización de pruebas periódicas de copias de seguridad. Lo anterior, deberá revisarse de conformidad con lo mencionado en el numeral 11.5. del presente informe.
8.17	A.12.4.4	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas.	**1**	Los relojes de los equipos de cómputo no están sincronizados con la hora local colombiana. Se tomó una muestra aleatoria de 41 equipos de la Sede de la Calle 69 y la 26, donde se evidenció que estos tienen retrasos de 3 y 4 minutos respecto a la hora local, adicionalmente un equipo de la Sede de la 69 tenía 7 horas adelantadas de diferencia.
8.18	A.9.2.3	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.	**2**	A través del directorio activo, se da acceso a programas de utilidad privilegiados. Los colaboradores de Capital de conformidad con las obligaciones contractuales o funciones establecidas del Manual de funciones, tienen acceso a los diferentes programas, para el caso de los contratistas el supervisor solicita al área de Sistemas los programas y servicios que se deben habilitar a este. Sin embargo, teniendo en cuenta que por requerimientos de cumplimiento de la misionalidad de Capital, existen equipos fuera del dominio que no cuentan con las políticas establecidas en materia de seguridad y privacidad de la información, lo cual se indicó en el seguimiento adelantado al Reporte a la Dirección Nacional de Derechos de Autor sobre el cumplimiento de las normas en materia de Derechos de Autor – Uso de Software, vigencia 2022, adelantado por la Oficina de Control Interno.

8.19	A.12.6.2	Instalación de software en sistemas operativos	Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	**2**	Se ajusta la calificación y análisis, teniendo en cuenta la respuesta remitida por el área. Lo anterior, se consolida en el **numeral 11.10** del presente informe.
8.23	A.12.2.1	Filtrado web	El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.	**1**	En Capital se tiene restringido el acceso a sitios pornográficos y juegos. Debido a que es un Sistema de Comunicación Pública no se restringe el acceso a redes sociales o plataformas de Streaming. Sin embargo, teniendo en cuenta el control A.12.2.1. Se requiere de la establecer una política formal que prohíba el uso de software no autorizado, atendiendo a la definición de política establecida en MANUAL PARA EL CONTROL DE DOCUMENTOS INSTITUCIONALES de Capital V5
8.24	A.10.1 A.10.1.1 A.10.1.2	Uso de criptografía	Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.	**1**	Los responsables indican que no se ha implementado este requisito normativo.
8.25	A.14.2.1	Ciclo de vida de desarrollo seguro	Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.	**2**	Se indica por los responsables que en el Manual Técnico de despliegue de implementación de software están documentadas las reglas para el ciclo de vida de desarrollo seguro, sin embargo, al revisar el Manual, en este falta incluir de conformidad con los requisitos del MSPI: a) definir la seguridad del ambiente de desarrollo; b) orientar la seguridad en el ciclo de vida de desarrollo del software: 1) definir la seguridad en la metodología de desarrollo de software; 2) establecer las directrices de codificación seguras para cada lenguaje de programación usado; c) definir los requisitos de seguridad en la fase diseño; d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto; e) establecer los depósitos seguros; f) definir la seguridad en el control de la versión; g) establecer el conocimiento requerido sobre seguridad de la aplicación; h) Definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.
8.27	A.14.2.5	Principios de arquitectura e ingeniería de sistemas seguros	Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.	**2**	Se indica por los responsables que en el Manual Técnico de despliegue de implementación de software están documentadas las reglas para el desarrollo de sistemas seguros, sin embargo, al revisar el Manual en este se indica que es específico para un sistema de Capital, en el objetivo general: *"Informar y especificar al usuario la instalación, estructura y conformación del sistema con el fin de que puedan hacer soporte, modificaciones y actualizaciones en general"*. De conformidad con el requisito normativo se debe documentar las generalidades o principios de arquitectura seguros para cualquier actividad de desarrollo de sistemas de información, por lo cual se deberá complementar el lineamiento y darle alcance en caso de ser necesario a los otros sistemas institucionales, teniendo en cuenta todos los requisitos definidos en la norma NTC ISO 27001.
8.30	A.14.2.7	Desarrollo contratado externamente	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas contratos externamente.	**2**	Los responsables indican que este ítem no aplica para Capital debido a "*el desarrollo de Capital es in house*", sin embargo, debe tenerse en cuenta que los colaboradores que desarrollan software para Capital no son funcionarios de planta, son personas externas por lo cual se deben establecer controles para dirigir, monitorear y revisar las actividades específicas con el desarrollo de sistemas. En las minutas contractuales se establecen cláusulas frente a los derechos de autor y conexos y la confidencialidad y uso de la información para todos los contratistas de Capital, sin embargo, debe revisarse por parte del (los) supervisor (es), ordenador del gasto, con el apoyo del área Jurídica si se requieren cláusulas adicionales que permitan asegurar los requisitos definidos en el MSPI: a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente; b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas; c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo;

					d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables; e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad; f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega; g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas; h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible); i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías; j) documentar eficaz del ambiente de construcción usado para crear entregables; k) establecer que la organización es responsable de conformidad con las leyes aplicables y con la verificación de la eficiencia del control.
8.31	A.12.1.4	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.	**3**	De conformidad con lo indicado por los responsables los entornos se encuentran separados, se encuentran en el mismo servidor pero cada uno tiene de manera independiente: directorios, bases de datos, archivos de configuración, sistema de logueo, que da acceso a un entorno distinto para cada uno. Lo anterior, se ha podido evidenciar por ejemplo en el desarrollo del ERP de plan de mejoramiento a cargo de la Oficina de Control Interno.
8.32	A.14.2.2	Gestión del Cambio	Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.	**3**	Durante septiembre de 2022 se implementó en el sistema de gestión el procedimiento Gestión de Cambios, en el cual se definen las actividades a seguir para implementar un cambio en la plataforma tecnológica de Canal Capital, con el fin de reducir el impacto y minimizar la interrupción en la prestación de los servicios tecnológicos.
8.33	A.12.7	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.	**1**	Para el periodo evaluado no se han realizado auditorías a los sistemas de información.

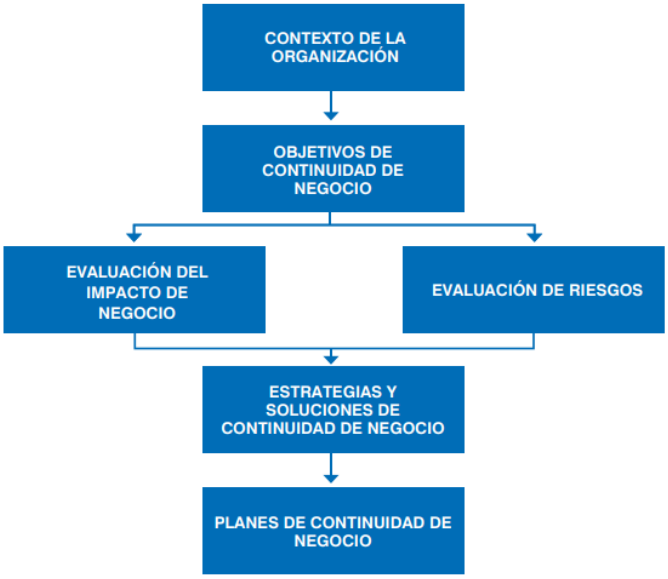
11.5. DOCUMENTOS GENERALES DEL PROCESO [RELACIONADOS CON EL MSPI]

Durante las pruebas realizadas se verificaron documentos vigentes en el sistema de gestión de Capital asociados a la implementación del Modelo de Privacidad y Seguridad de la Información e implementación de controles de la ISO 27001, a continuación, se presentan documentos donde se evidenciaron debilidades y oportunidades de mejora de conformidad con lo solicitado en los diferentes requisitos normativos y el uso de formatos del proceso:

Tabla 3. Documentación proceso Sistemas

Código	Nombre	Versión	Observaciones
AGRI-SI-MN-001	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	2	Documento actualizado a su versión 2 en diciembre de 2021, en el manual no se establece cuál es el objetivo del documento, se establecen por el contrario cuáles son los objetivos del Sistema de Gestión de Seguridad de la Información, por lo que debe revisarse y complementarse, ya que este no corresponde con el propósito de lo que se busca con la formulación del documento. De igual manera, respecto a la redacción del objetivo se recomienda tener en cuenta las diferentes metodologías existentes. En el manual no se establece cuál es el alcance de aplicación de los lineamientos establecidos en el documento. El documento no se encuentra articulado con otros lineamientos existentes dentro del sistema de gestión, por ejemplo, se indica que hay Procedimientos y Mecanismos que soportan el SGSI, pero no se indican cuáles son estos procedimientos o dónde se pueden consultar; se da la definición de riesgo, vulnerabilidad y amenaza pero no se indica que Capital cuenta con una matriz de riesgos de seguridad digital donde se está minimizando la afectación de esos tres factores; se indica que existen tres componentes para el diseño del SGI para el componente uno hay una lista de documentos pero no indica si Capital ya cuenta con estos o están en proceso de construcción, para los componentes dos y tres no hay ninguna información respecto a qué son o de su implementación en la entidad.
AGRI-SI-MN-006	MANUAL DE POLÍTICAS COMPLEMENTARIAS	3	Documento actualizado a su versión 3 en diciembre de 2021. Frente a este documento es importante su socialización y divulgación permanente a todas las áreas y colaboradores de la entidad, dado que tiene gran número de políticas y lineamientos a aplicar que son desconocidas por su falta de socialización [Teniendo en cuenta lo observado durante las pruebas adelantadas en sitio los días 16 y 24 de agosto 2023]. Es necesario complementar el manual de acuerdo con lo verificado en los controles de la ISO 27001: • Respecto a los roles y responsabilidades se recomienda que se complementen las políticas frente a escenarios de acoso, difamación, suplantación de identidad, compras no autorizadas de manera articulada con la documentación existente en materia de contratación y de ingreso, mantenimiento y retiro de personal emitidos por el área de Talento Humano. • Complementar la responsabilidad que tiene el área de Recursos Humanos en los siguientes numerales: - Numeral 5.2.2 Durante la Ejecución del Empleo: El área de RH debe notificar al área de Sistemas los periodos de vacaciones y/o licencias de funcionarios de planta para desactivar los servicios y acceso a la información durante la ausencia del funcionario. - Numeral 5.2.3 Terminación y Cambio de Empleo: El área de RH debe notificar al área de Sistemas de la terminación del contrato de un funcionario de planta, ya que no hay una inactivación automática de los servicios como en caso de los contratistas que tienen una fecha de terminación estipulada. • Revisar las políticas como de no ingerir alimentos y bebidas en los puestos de trabajo, indicando entonces los lugares permitidos y adecuados para hacerlo en las instalaciones de la Calle 26 y la Casa de la 69 y comunicando esta política en todas las áreas de trabajo, publicar esta información en afiches, carteles, protectores de pantalla etc. • Estandarizar los tiempos de bloqueo seguro en los equipos pidiendo usuario y contraseña, para evitar la exposición a la consulta de información confidencial, robo de información, eliminación de información.
AGRI-SI-GU-009	GUÍA DE BORRADO SEGURO DE INFORMACIÓN	2	Documento actualizado a su versión 2 en diciembre de 2022. En la guía se definen los lineamientos adoptados por la entidad para borrar de forma segura la información, indicando los diferentes métodos que existen y sus ventajas y desventajas; sin embargo, se recomienda definir en la guía quién ejercerá la responsabilidad final de verificar que la información se haya eliminado segura y

Código	Nombre	Versión	Observaciones
			definitivamente, ya que no se establece ese punto de control, así como el documento idóneo para soportar la ejecución de las actividades relacionadas.
AGRI-SI-PD-014	PROCEDIMIENTO COPIAS DE SEGURIDAD	10	Documento actualizado a su versión 10 en mayo de 2021. Teniendo en cuenta la respuesta dada por los responsables, no se cuenta con una política de copias de seguridad sino con un procedimiento; sin embargo, de conformidad con lo requerido en el control A.12.3.1. Copias de seguridad de la información, se debe definir una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias, dependiendo de la necesidad de la entidad respecto al tipo de información, adicionalmente se debe tener en cuenta la definición y características que debe tener una política de conformidad con lo definido en el Manual para el control de documentos institucionales, versión 5.
AGRI-SI-PL-002	PLAN DE CONTINUIDAD DEL NEGOCIO	1	Documento creado el 18 de enero de 2021. De conformidad con el listado de los componentes y recursos informáticos que conforman los sistemas de información presentado en el documento, se realizó la verificación de software, tecnología e infraestructura y servicios descritos en el mismo con el objetivo de verificar si existían y sigue vigentes su uso en Capital, de lo anterior se evidencio que el numeral 2.1, debe actualizarse en su totalidad, debido a: • **Tecnología, infraestructura tecnológica:** De los doce equipos presentado en el plan de continuidad, ocho tuvieron modificaciones y mejoras, las marcas, cantidades y capacidad que se describen en el documento ya no corresponden a la realidad de los equipos. • **Software:** De los diecisiete que se indican como activos, dos ya no se utilizan (SIMED y Assets Invgate); el sistema Symantec Backup Exec 2020 cambio de nombre a Veritas Backup; existe el Windows Server Data Center server 2016, sin embargo, se usa también versiones de 2019; adicionalmente deben incluirse los desarrollos in house que se han realizado para los diferentes procesos de Capital. Así mismo, uno de los objetivos específicos del plan es el de *"asignar responsabilidades al personal designado"*, en los casos de emergencia identificados no se define quién debe hacer los reportes o activar los protocolos para mitigar o eliminar los riesgos producto de la emergencia presentada, tampoco se define cuál es la responsabilidad de los colaboradores de Capital ante los casos de emergencia. De igual manera, se evidencian inconsistencias en el numeral 3.2.1 criterios de la matriz de riesgos, donde se indica que se relacionan las actividades que se deben realizar con el objeto de prever, mitigar o eliminar los posibles riesgos conocidos, esta lista de riesgos debe complementarse con los riesgos identificados en la matriz de seguridad digital. En el numeral 5 se establecen datos de contacto para el escalamiento interno en los cuales se relaciona una persona que ya no está vinculada a la entidad. Adicionalmente, no hay datos para el reporte de los casos que requieren escalamiento externo. Por lo anterior, se hace necesario adelantar la verificación y actualización del plan de continuidad vigente, teniendo en cuenta los requerimientos de la ISO 23301:2019; por lo que es importante que se adelante la estructuración de un documento que cuente con: un alcance, referencias normativas aplicables, términos y condiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora, enmarcados en los conceptos de:

Código	Nombre	Versión	Observaciones
			 **Fuente:** Guía de implantación de la ISO 22301:2019.
AGRI-SI-PD-020	GESTIÓN DE CAMBIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	1	Este procedimiento fue creado en septiembre de 2022. Fue evaluado durante la entrevista realizada a los Profesionales de Sistemas el día 16 de agosto de 2023, durante la prueba realizada se indicó que las actividades descritas en el procedimiento no se hacen a través del "Módulo soporte mesa de ayuda", ya que este aún no ha sido activado en el ERP y se encuentra en proceso de elaboración, por ende, el procedimiento no corresponde a como actualmente se están gestionando los cambios en la plataforma tecnológica de Capital. Se debe tener en cuenta que un procedimiento describe la secuencia lógica de las actividades que se ejecutan en un proceso, no de las que se tienen planeadas ejecutar en un futuro una vez esté la mesa de ayuda, por ende, es necesario que el procedimiento corresponda al cumplimiento de actividades que sí se ejecutan, teniendo en cuenta que el tiempo de implementación del ERP es incierto.
AGRI-SI-MN-005	MANUAL DE GESTIÓN DE USUARIOS	2	Documento actualizado en la vigencia 2021, sin embargo, se hace necesario que se actualice de conformidad con las debilidades identificadas en el marco de la evaluación de los controles establecidos en la norma ISO 27001, en lo referente a la documentación de las actividades adelantadas, consolidación de soportes de actas generadas de entrega de servicios TIC, actividades de asignación, modificación, eliminación, suspensión de cuentas a que haya lugar por incapacidades, vacaciones, licencias, entre otros eventos y que a su vez, se adelanten de conformidad con lo establecido en el procedimiento general de dicho documento. Lo indicado, en atención a lo referenciado en el numeral 11.4. del presente informe.
AGRI-SI-PL-003	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	2	Se recomienda adelantar el monitoreo y seguimiento por parte del área respecto al esquema de actividades establecidas en el documento, respecto a las fases de implementación y evaluación y seguimiento de manera que sean coherentes con el reporte adelantado a los indicadores formulados.
AGRI-SIPL-004	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	3	El documento si bien articula otros lineamientos establecidos en la política de administración de riesgos y el manual de administración de riesgos, el documento no indica la metodología para mitigación de riesgos de seguridad y privacidad, así como tampoco se relacionan los recursos, presupuesto requerido, medición del plan formulado, de manera que se pueda verificar el cumplimiento de las actividades programadas para la vigencia. Lo mencionado, en atención a lo referenciado en el numeral 11.4. del presente informe.

Código	Nombre	Versión	Observaciones
AGRI-SI-PL-005	PLAN DE SENSIBILIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	2	El documento articula actividades del plan de sensibilización, sobre el cual se recomienda adelantar la identificación del universo de actividades, así como la herramienta de monitoreo y seguimiento de manera que se pueda evidenciar la ejecución de lo formulado de conformidad con el tiempo y recursos requeridos. Lo mencionado, en atención a lo referenciado en el numeral 11.4. del presente informe.

11.6. PLAN ESTRATÉGICO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN – PETI

El Plan Estratégico de Tecnologías de la Información – PETI se compone de un documento maestro o pdf denominado AGRI-SI-PL-001 Plan Estratégico de Tecnologías de la Información – PETI donde se consigna la planeación estratégica del cuatrienio 2020 – 2024, y se detalla las estrategias adoptadas por Capital en materia de TI y Gobierno TI, Infraestructura Tecnológica, Gestión de Seguridad y Privacidad de la Información y Sistemas de Información, Datos y Servicios Digitales, adicionalmente se elabora un documento en Excel denominado "hoja de ruta de ejecución – PETI", dónde se establecen los proyectos a ejecutar en cada vigencia y el presupuesto asignado.

El documento maestro AGRI-SI-PL-001 fue actualizado a su versión 3 en octubre de 2022, y la Hoja de ruta fue actualizada en junio 13 de 2023, incluyendo los proyectos a adquirir con los recursos Futic en la vigencia 2023; sin embargo, no se evidencia que se haya realizado una actualización paralela de ambos documentos, teniendo en cuenta que en numeral 5.6.1 del pdf se realiza un análisis del plan financiero de la vigencia. Adicionalmente, no es posible determinar los ajustes realizados, así como las versiones, dado que estos datos no se incluyen en el documento [Hoja de ruta - Excel]:

Ilustración 4. Análisis PETI

5.6.1 Análisis de presupuesto

El Plan Financiero para la vigencia 2022 asciende a $ 43.457.809.000 presentando un incremento del 7% con respecto a la apropiación disponible con corte a 30 de agosto de 2021, el cual se encuentra clasificado en grandes rubros presupuestales de ingreso y gasto[5]

La descripción del presupuesto de inversión 2022 se detalla en la siguiente tabla:

Tabla 8. Presupuesto de Inversión

Ingresos Corrientes	**38.065.835.000,00**
Venta de bienes y servicios	11.156.722.000,00
Transferencias Corrientes	26.909.113.000,00

Tabla 10. Gastos de Funcionamiento

FUNCIONAMIENTO	PRESUPUESTO 2021	PRESUPUESTO 2022
GASTOS DE FUNCIONAMIENTO	**769.009.986,88**	**561.358.300**
Remuneración Servicios Técnicos	64.464.000	64.464.000
Apoyo Técnico - Infraestructura TIC	29.664.000	28.100.000
Apoyo Técnico - Sistemas TIC	34.800.000	32.400.000
Apoyo Técnico - Sistemas TIC	0	23.700.000
Gastos de Computador	417.573.625	223.222.200
Suministro de Insumos y partes.	93.359.200	64.240.008
Licencias (Antivirus, ADOBE,Oficce y servidores - Vmware)	72.000.000	143.672.598
Mantenimiento preventivo y correctivo de equipos, Datacenter y vmware.	160.062.000	126.522.200
Certificados digitales	583.522	2.000.000
Mantenimiento de Software Ordpago (Soporte técnico, desarrollo y mantenimiento Ordpago y kárdex)	52.450.896	53.700.000
Software Contable - mantenimiento y actualización SIIGO - Software Contable SIMED	4.374.099	6.000.000

Fuente: http://intranet.canalcapital.gov.co/intranet/docdowncc/DocSistema/2022/Plan/AGR-SI-PL-001%20PLAN%20ESTRATEGICO%20DE%20TECNOLOGIAS%20DE%20LA%20INFORMACION%20-%20PETI.pdf

El cumplimiento del PETI se encuentra incluido dentro de los proyectos de inversión de Capital, corresponde a la meta 3 del proyecto 7511: "Implementar el 100 % de actividades asociadas al Plan Estratégico de Tecnologías de la Información - PETI El desarrollo de la actividad implica el diseño, elaboración, ejecución y seguimientos al Plan de Tecnologías de Información y las comunicaciones - PETI, orientadas al fortalecimiento y adquisición de equipos requeridos para la entidad".

Durante los seguimientos realizados a los proyectos de inversión de Capital en la vigencia 2022 y el primer trimestre de la vigencia 2023, se solicitó a los responsables de hacer seguimiento a la ejecución del PETI la elaboración de una herramienta que permitiera soportar documentalmente los avances de la meta física y presupuestal reportados de manera trimestral, lo anterior, teniendo en cuenta que los reportes se hacen al área de Planeación de manera cualitativa y general, no se especifica para cada uno de los proyectos de la Hoja de ruta del PETI su nivel de avance físico y de recursos financieros, desde el área de Sistemas se propuso elaborar un plan de trabajo, como herramienta de seguimiento a la ejecución del plan. Se solicitó la herramienta de seguimiento a la fecha, evidenciando las siguientes debilidades:

Ilustración 5. Herramienta seguimiento PETI

PLAN DE TRABAJO SISTEMAS 2023																			SEGUIMIENTO							
Proyecto PETI	Item	Actividades	Responsable	2023												ESTATUS	OBSERVACIONES	Programado	Asigado por actividad	Tema	Cantidad de actividades	Ejecución			
				Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre							1 trimestre (en-fe-mar)	2 trimestre (abr-may-jun)	3 trimestre (jul-ago-sep)	4 trimestre (oct-nov-dic)
Renovación Tecnológica	1	Administrar pool IPv6 y actualizar registros de RIPXI (infraestructura de clave pública de recursos) IPV6.	Administrador de infraestructura - Apoyo de infraestructura													En ejecución		95%	4%	Actividades PETI (27 act)	27	24%	24%		
	2	Gestionar y mantener actualizado el inventario de la infraestructura servicios TIC, Documento CMDB.														En ejecución		95%	24%	Actividades Seguridad (8 act)	8	24%	24%		
	3	Administrar y actualizar protocolo SNMP y VMI en equipos servidores y comunicaciones.														En ejecución		95%	48%	Actividades Riesgos Seguridad (2)	2	24%	24%		
	4	Gestionar y actualizar topologia lógica y enrutamiento IPv4/IPV6.														En ejecución									
	5	Administrar y actualizar servicio de monitoreo PRTG (software de monitoreo de red).														En ejecución									
	6	Gestionar y actualizar capacidad de los servicio TIC.														En ejecución									
	7	Administrar y actualizar granja de servidores.														En ejecución									
	8	Gestionar los accesos remotos para la administracion de la infraestructura TIC.														En ejecución									
	9	Administrar y disponer los segmentos de red (VLAN) para la zede 1 y 2 de acuerdo a la necesidad de la operación.														En ejecución									
	10	Administrar y soportar la interconexion de los servicios TIC.														En ejecución									
	11	Gestionar y soportar el cableado estructurado puntos de datos y electricos.														En ejecución									
	12	Administrar y soportar centros de datos, servidor de backups, servidor de virtualizacion de servidores.														En ejecución									
	13	Implementar servidores de respaldo de File server y servidores de escritorios en centro de datos calle 69.														No iniciado	iniciar ya que no adquirieron los servidores y el amacenamiento para la sede								
	14	Administrar y soportar el servicio de seguridad perimetral Firewall														En ejecución									
	15	Implementar controles de seguridad informatica, para la operacion de servicios TIC.														En ejecución									

Fuente: Plan de trabajo sistemas 2023

a. Se le incluyeron columnas para hacer seguimiento a cada actividad, sin embargo, la información no se ha diligenciado para la totalidad de las actividades y/o proyectos.

b. En la herramienta no se incluyeron los proyectos de la Hoja de ruta de PETI, que tienen recursos asignados para la vigencia 2023, como algunos ejemplos resaltados en amarillos a continuación:

Ilustración 6. Hoja ruta PETI

CENTRO DE DATOS Y CONTINGENCIA				
Proyecto	Costo Estimado	PRESUPUESTO		
		2021	2022	2023
Data center tier2	255000000		$ 90.000.000	$ -
		$ 50.000.000	$ 50.000.000	$ -
Monitoreo IPV6	80400000	$ 80.400.000	$ 84.000.000	$ 74.675.000
		$ 165.000.000	$ -	$ 81.390.000
Data center de respaldo CDP	158000000	$ 73.000.000	$ 85.000.000	$ 96.754.780
		$ 198.000.000	$ 45.000.000	$ -
Renovación tecnológica	262800000	$ 63.800.000	$ 97.000.000	
	$837.590.000,00	**$630.200.000,00**	**$451.000.000,00**	**$252.819.780,00**
SOFTWARE Y GESTION DOCUMENTAL				
Proyecto	Costo Estimado	PRESUPUESTO		
		2021	2022	2023
Sistema integrado de gestión documental	100000000	$ 51.200.000	$ 50.000.000	$ -
		$ 100.000.000	$ 100.000.000	$ 158.760.000
	$510.000.000,00	**$151.200.000,00**	**$150.000.000,00**	**$158.760.000,00**
AREA TECNICA				
CONTRIBUCIONES				
Proyecto	Costo Estimado	PRESUPUESTO		
		2021	2022	2023
Sistema de contribuciones por RF	$350.000.000,00	$0,00		$ -
Infraestructura para ingesta	$120.000.000,00	$35.000.000,00		$ 35.000.000
Electrónica de procesamiento	$105.000.000,00	$35.000.000,00		$ -
Sistema de contrribuciones por IP	$240.000.000,00	$30.000.000,00	$ 71.835.140	$ 35.000.000
	$815.000.000,00	**$100.000.000,00**	**$71.835.140,00**	**$70.000.000,00**
PRODUCCIÓN				
Proyecto	Costo Estimado	PRESUPUESTO		
		2021	2022	2023
Sistemas de reproducción	$250.000.000,00	$ -		$ -
Dispositivos de grabación y accesorios	$280.000.000,00	$ 35.000.000		$ 35.000.000

Fuente: Hoja de Ruta del PETI - Proyectos con ejecución en la vigencia 2023

c. Teniendo en cuenta que a la meta presupuestal también se le realiza seguimiento, es importante incluir una columna con los recursos asignados a cada proyecto e ir realizando seguimiento a la ejecución presupuestal según la periodicidad del reporte de la información.

d. No se indica cuál es la evidencia que soporta el cumplimiento de cada actividad.

Por lo anterior, se hace necesario mejorar la herramienta de seguimiento incluyendo la información requerida para poder soportar documentalmente el avance de cada uno de los proyectos de la hoja de ruta del PETI, así como mantener actualizada la información y relacionar los soportes de cumplimiento de cada actividad.

11.6.1 PUBLICACIÓN DEL PETI EN EL BOTÓN DE TRANSPARENCIA A MÁS TARDAR EL 31 DE ENERO DE CADA VIGENCIA

De conformidad con el Decreto 612 de 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado" de la Presidencia de la República, se establece:

> *"Artículo 2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar*

los planes institucionales y estratégicos que se relacionan a continuación y publicarlos, en su respectiva página web, a más tardar el 31 de enero de cada año"

"**2.2.22.3.14. *Integración de los planes institucionales y estratégicos al Plan de Acción.*** Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:

1. Plan Institucional de Archivos de la Entidad PINAR
2. Plan Anual de Adquisiciones
3. Plan Anual de Vacantes
4. Plan de Previsión de Recursos Humanos
5. Plan Estratégico de Talento Humano
6. Plan Institucional de Capacitación
7. Plan de Incentivos Institucionales
8. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
9. Plan Anticorrupción y de Atención al Ciudadano
10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI
11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
12. Plan de Seguridad y Privacidad de la Información

Revisado el plan de acción de Capital para la vigencia 2023, no se evidencia la publicación e integración del Plan Estratégico de las Tecnologías de Información - PETI formulado para la vigencia 2023 al plan de acción, se evidencia que se publicaron indicadores para medir el avance de algunas actividades asociadas al PETI para la vigencia 2023, incumpliendo con lo establecido en el artículo 2.2.22.3.14:

Objetivo: *Establecer la planificación estratégica de las tecnologías de la información de Capital, para el periodo comprendido entre el 2021 y 2024, acordes con las necesidades de la Entidad y los lineamientos de la Política de Gobierno Digital, a partir de la planeación estratégica apalancada en las tecnologías de la información y la implementación de políticas de gestión y desempeño institucional que contribuya al logro de los objetivos institucionales, apoyando todas las actividades y proyectos de Capital.*

Versión del plan: *2*

Fecha de Aprobación: *31/1/2023*

Plan de actividades							
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		Ponderación
					INICIO	FIN	100%
1	Actualizar el PETI y hoja de ruta para la vigencia del 2023	Sistemas	Documento PETI y Hoja de ruta 2023	100%	1/3/2023	30/10/2023	30%
2	LDAP y GOOGLE	Sistemas	Funcionando los servicios	80%	1/4/2023	30/12/2023	10%
3	Consolidación backup sede de la calle 69	Sistemas	Backup Sede Calle 69	80%	1/3/2023	30/12/2023	10%
4	Almacenamiento Intranet	Sistemas	Almacenamiento Data Intranet	80%	1/3/2023	30/12/2023	10%
5	Actualización de firewall	Sistemas	Actualización del Firewall	80%	1/2/2023	30/12/2023	10%
6	Desarrollar y mejorar los módulos administrativos el marco del sistema de gestión empresarial	Sistemas	Módulos administrativos implementados del ERP	100%	1/2/2023	30/12/2023	30%

Fuente: Plan de acción institucional V2

Se evidencia que Capital no tiene un lineamiento que indique que se debe realizar la publicación del PETI por parte de los responsables en la guía: LINEAMIENTOS PARA PUBLICACIÓN DE INFORMACIÓN EN LA

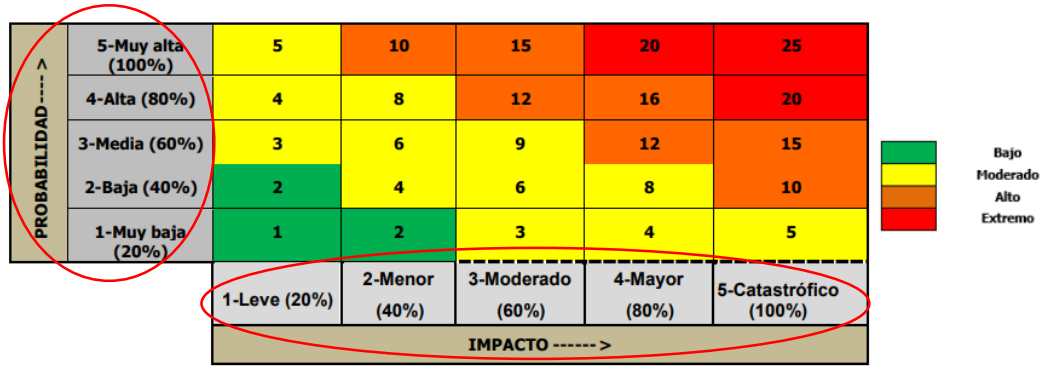
SEDE ELECTRÓNICA – V5, ni se cuenta con un espacio en el botón de transparencia para hacer la publicación e integración de los planes indicados en del Decreto 612 de 2018.

11.7. RIESGOS DE SEGURIDAD DIGITAL

Capital adoptó la matriz de riesgos de seguridad digital durante la vigencia 2022 y durante la ejecución de la auditoría (el 16 de junio de 2023) se actualizó a la versión 2, una vez evaluados los controles del numeral 11.4 y de conformidad con los lineamientos para la gestión del riesgo de Capital: Manual Metodológico para la Administración del riesgo V3 y política de administración del riesgo V8, se evidenciaron las siguientes debilidades:

a. La política de administración del riesgo definió la escala de calificación de los niveles de probabilidad e impacto con el fin de establecer las escalas para el tratamiento e implementarlas en las diferentes matrices de riesgos como se muestra a continuación:

7.1. NIVELES DE SEVERIDAD DEL RIESGO



Fuente: Política de administración del riesgo V8

Se evidencia que estas escalas difieren de las que se están implementando en la matriz de riesgos de seguridad digital:

Nivel de Probabilidad		Descripción
Raro	1	El riesgo ocurre rara vez en la entidad.
Improbable	2	El riesgo ocurre en ocasiones específicas en la entidad
Posible	3	El riesgo ocurre con cierta periocidad en la entidad.
Probable	4	El riesgo ocurre frecuentemente en la entidad.
Casi Seguro	5	El riesgo ocurre inminentemente en la entidad.

Nivel de Impacto		Descripción
Insignificante	1	Si se presenta, puede tener consecuencias en un grupo de funcionarios de manera interna y controlada.
Menor	2	Si se presenta, puede tener impacto leve en la entidad, reparable en el corto plazo.
Moderado	3	Si se presenta, puede tener impacto medio en la entidad de manera local o interna.
Mayor	4	Si se presenta, se puede tener impacto alto en la entidad a nivel del sector.
Catastrófico	5	Si se presenta, puede tener impacto catastrófico en la entidad de orden nacional o internacional.

Por lo anterior, se está incumpliendo con la escala establecida para calcular el impacto y la probabilidad, ya que no se estableció una escala diferencial para los riesgos de seguridad digital.

b. De conformidad con el control A.11.2.4 de la ISO 27001:2013, se deben diseñar e implementar controles contra amenazas físicas y ambientales, en la matriz de riesgo se encuentran identificadas amenazas físicas, sin embargo, amenazas de tipo ambiental como fenómenos climáticos, físicos, inundación, sísmicos, meteorológicos no se han documentado, ni formulado controles para minimizar el riesgo de afectaciones en la privacidad y seguridad de la información.

c. De conformidad con el control A.11.2.6 de la ISO 27001:2013, se debe garantizar la seguridad de los activos fuera de las instalaciones de Capital que pueden contener información sensible de la entidad, para aquellos colaboradores que ejerzan su función en la modalidad de teletrabajo, trabajo remoto o lugares temporales, dada la misionalidad de Capital se debe realizar una valoración de riesgos para controlar los equipos que salen de las instalaciones estableciendo controles adecuados como: No dejarlos sin vigilancia en lugares públicos, usar gabinetes de archivo con llave, aplicar la política de escritorio limpio en casa, establecer controles de acceso para computadores, llevar una cadena de custodia de los equipos etc., de lo anterior no se evidencia su identificación en la matriz de riesgos de seguridad digital y/o documentos asociados a las actividades de seguridad y privacidad de la información que se adelantan en Capital.

11.8. INDICADORES DEL PROCESO

Teniendo en cuenta lo definido en la Guía de indicadores de Gestión de seguridad de la información del MinTic se deberán contemplar las etapas de identificación del objeto de la medición, definición de las variables, selección de indicadores y calidad de datos y diseño del indicador que permitan medir la efectividad, eficiencia y eficacia de los componentes aplicables del modelo de operación en el marco de la seguridad y privacidad de la información, así como tener insumos para la mejora continua y toma de decisiones.

Dado que de los (15) indicadores definidos en la guía en Capital, no se identifica ninguno, sino que por el contrario hacen parte de las actividades de los diferentes planes construidos, se mencionan las debilidades identificadas, así como recomendaciones que le permitan al área adelantar la mejora correspondiente a dicho componente, de la siguiente manera:

11.8.1. Indicadores vigencia 2022

Para la vigencia 2022 se adelantó la formulación de tres indicadores, los cuales se enmarcan en el cumplimiento de los planes estratégicos de tecnologías de la información – PETI, plan de seguridad y privacidad de la información y plan de tratamiento de riesgos de seguridad y privacidad de la información como se observa a continuación:

Ilustración 7. Indicadores 2022

Códi	Proyecto / Pla	Indicador	Fórmula del indicador		Meta 2022		Liderazgo estratégic	Proceso relacionado
			Numerador	Denominado	Magnitu	Descripción		
3.7.3	Plan Estratégico de Tecnologías de la Información - PETI 2022 (Anexo 2)	Cumplimiento de actividades del Plan Estratégico de Tecnologías de la Información - PETI 2022	Porcentaje de avances de las acciones programadas en el Plan Estratégico de tecnologías de la información - PETI	Porcentaje programado de acciones del Plan Estratégico de tecnologías de la información - PETI para la vigencia	95%	Ejecutar como mínimo el 95% de las actividades programadas en el plan de tecnologías de la información (Plan Estratégico de Tecnologías de la Información - PETI).	Subdirección Administrativa	Gestión de recursos administrativos.
3.7.4	Plan de Seguridad y Privacidad de la Información 2022 - PSPI (Anexo 3)	Cumplimiento de actividades del Plan de seguridad y privacidad de la información	Porcentaje de avances de las acciones programadas en el Plan de seguridad y privacidad de la información	Porcentaje programado de acciones del Plan de seguridad y privacidad de la información para la vigencia	95%	Ejecutar como mínimo el 95% de las actividades programadas en el Plan de Seguridad y Privacidad de la Información	Subdirección Administrativa	Gestión de recursos administrativos.
3.7.5	Plan de tratamiento de riesgos de seguridad y privacidad de la información 2022 - PTRSI (Anexo 4)	Cumplimiento de actividades del Plan de tratamiento de riesgos de seguridad y privacidad de la información	Porcentaje de avances de las acciones programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Porcentaje programado de acciones del Plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia	95%	Ejecutar como mínimo el 95% de las actividades programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Subdirección Administrativa	Gestión de recursos administrativos.

Así mismo, cada indicador se ejecuta en el marco de las actividades formuladas en el plan como se presenta a continuación:

a. Plan Estratégico de Tecnologías de la Información

Compuesto por cinco (5) actividades, de las cuales se reporta información y soportes del desarrollo y mejora de los módulos ERP de Control interno, Recursos Humanos y gestión documental, así como del reporte del equipo de seguridad perimetral firewall y servicio del centro de datos; sin embargo, no se evidencian los informes mensuales de monitoreo del protocolo IPV6 e implementación del robot de Backup LTO8, registrando el cumplimiento del 100% de la meta formulada. Lo anterior, denota debilidades en el reporte, verificación y acompañamiento de la medición de actividades.

Plan de actividades							
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		Ponderación
					INICIO	FIN	
							100,00%
1	Monitoreo del protocolo IPV6	Sistemas	Informes mensuales de monitoreo	80%	1/2/2022	30/12/2022	30%
2	Data center con replicación tier 2 en la sede principal	Sistemas	Data center con replicación implementado	80%	1/4/2022	30/12/2022	10%
3	Adquisición e implementación del robot de backup LTO8 en el data center principal	Sistemas	Robot de backup LTO8 implementado	100%	1/3/2022	30/12/2022	15%
4	Adquisición e implementación del sistema de seguridad perimetral firewall para alta disponibilidad	Sistemas	Firewall del alta disponibilidad adquirido e implementado	80%	1/4/2022	30/12/2022	15%
5	Desarrollar y mejora de los módulos administrativos el marco del sistema de gestión empresarial	Sistemas	Módulos administrativos implementados del ERP	100%	1/3/2022	30/12/2022	30%

b. Plan de seguridad y privacidad de la información

El cual se compone de cuatro (4) actividades enmarcadas en la implementación de políticas, procedimientos, lineamientos, instructivos, sensibilización en materia de SGSI, controles de seguridad y alistamiento de la certificación; sin embargo, teniendo en cuenta que no se define el universo de la documentación a actualizar, así como tampoco se define el número de estrategias y controles a implementar durante la vigencia, no es posible determinar que se ejecute a cabalidad lo formulado. De

igual manera, no se evidencian reportes sobre el documento de alistamiento de certificación de la ISO 27001.

Plan de actividades							
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		
					INICIO	FIN	Ponderación
							100,00%
1	Documentar políticas, procedimientos, lineamientos, instructivos, etc. Asociados al MSPI y Gobierno Digital.	Sistemas	Documentos publicados en la intranet de la entidad	100%	1/3/2022	30/12/2022	20%
2	Implementar el plan de sensibilización del SGSI.	Sistemas	Estrategias implementadas del SGSI.	100%	1/3/2022	30/9/2022	30%
3	Implementar controles de seguridad en la plataforma tecnológica de la entidad	Sistemas	Controles implementados en la plataforma tecnológica	100%	1/2/2022	30/12/2022	40%
4	Alistamiento para la certificación en ISO 27001 de un proceso de la entidad.	Sistemas	Documento de gestión	100%	1/4/2022	30/12/2022	10%

c. Plan tratamiento de riesgos de seguridad y privacidad de la información

Se define por una (1) actividad enmarcada en la implementación de la matriz de riesgos de seguridad digital, identificando dos (2) riesgos respecto al acceso indebido o mal intencionado a los recursos tecnológicos de Capital, así como de interrupción de servicios, sin contemplar riesgos de pérdida de información.

Plan de actividades							Seguimiento
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		Ponderación
					INICIO	FIN	
							100,00%
1	Implementación de la matriz de riesgos de seguridad digital	Sistemas	Matriz de riesgos de seguridad digital	100%	1/3/2022	30/12/2022	100%

11.8.2. Indicadores vigencia 2023

Para la vigencia 2023, se mantienen los indicadores de la vigencia 2022 con ajustes de actividades, como son:

Ilustración 8. Indicadores 2023

Correspondencia con ODS	Objetivo estratégico		Código	Proceso	Indicador	Tipo de Indicador	Fórmula del indicador		Unidad de medición	Tendencia
							Numerador	Denominador		
9. Industria, innovación e infraestructura. 16. Paz, justicia e instituciones sólidas.	OE_3	3. Generar una cultura digital y de gestión del conocimiento para la optimización de los procesos internos y externos.	3.7.4	Gestión de recursos administrativos.	Cumplimiento de actividades de la hoja de ruta del Plan Estratégico de Tecnologías de la Información - PETI 2023.	2 Eficiencia: Uso de los recursos.	Porcentaje de avances de las acciones programadas en el Plan Estratégico de tecnologías de la información - PETI	Porcentaje programado de acciones del Plan Estratégico de tecnologías de la información - PETI para la vigencia	Porcentaje (%).	1 Creciente: El resultado tiende a crecer en el tiempo
9. Industria, innovación e infraestructura. 16. Paz, justicia e instituciones sólidas.	OE_3	3. Generar una cultura digital y de gestión del conocimiento para la optimización de los procesos internos y externos.	3.7.5	Gestión de recursos administrativos.	Cumplimiento de actividades del Plan de seguridad y privacidad de la información 2023.	2 Eficiencia: Uso de los recursos.	Porcentaje de avances de las acciones programadas en el Plan de seguridad y privacidad de la información	Porcentaje programado de acciones del Plan de seguridad y privacidad de la información para la vigencia	Porcentaje (%).	1 Creciente: El resultado tiende a crecer en el tiempo
9. Industria, innovación e infraestructura. 16. Paz, justicia e instituciones sólidas.	OE_3	3. Generar una cultura digital y de gestión del conocimiento para la optimización de los procesos internos y externos.	3.7.6	Gestión de recursos administrativos.	Cumplimiento de actividades del Plan de tratamiento de riesgos de seguridad y privacidad de la información 2023.	2 Eficiencia: Uso de los recursos.	Porcentaje de avances de las acciones programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Porcentaje programado de acciones del Plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia	Porcentaje (%).	1 Creciente: El resultado tiende a crecer en el tiempo

a. Plan Estratégico de Tecnologías de la Información

Compuesto por seis (6) actividades enmarcadas en la actualización del PETI, funcionamiento de recursos LDP y Google, consolidación del Backup de la calle 69, actualización del firewall y desarrollo y mejora de los módulos de ERP que se vienen construyendo de conformidad con las necesidades de Capital.

Plan de actividades							
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		Ponderación
					INICIO	FIN	100%
1	Actualizar el PETI y hoja de ruta para la vigencia del 2023	Sistemas	Documento PETI y Hoja de ruta 2023	100%	1/3/2023	30/10/2023	30%
2	LDAP y GOOGLE	Sistemas	Funcionando los servicios	80%	1/4/2023	30/12/2023	10%
3	Consolidación backup sede de la calle 69	Sistemas	Backup Sede Calle 69	80%	1/3/2023	30/12/2023	10%
4	Almacenamiento Intranet	Sistemas	Almacenamiento Data Intranet	80%	1/3/2023	30/12/2023	10%
5	Actualización de firewall	Sistemas	Actualización del Firewall	80%	1/2/2023	30/12/2023	10%
6	Desarrollar y mejorar los módulos administrativos el marco del sistema de gestión empresarial	Sistemas	Módulos administrativos implementados del ERP	100%	1/2/2023	30/12/2023	30%

b. Plan de seguridad y privacidad de la información

Se mantienen tres (3) de las cuatro (4) actividades formuladas, haciendo ajuste de la actividad de la ISO 27001, proyectando la ejecución del plan de mejoramiento de la auditoría adelantada por la oficina de control interno durante la vigencia anterior.

Plan de actividades							
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		Ponderación
					INICIO	FIN	100%
1	Documentar políticas, procedimientos, lineamientos, instructivos, entre otros.	Sistemas	Documentos publicados en la Intranet de la entidad	100%	1/1/2023	30/12/2023	20%
2	Continuar con la implementación de las estrategias de sensibilización, apropiación y uso de SGSI.	Sistemas	Estrategias implementadas del SGSI	100%	1/1/2023	30/12/2023	20%
3	Implementar y mejorar los controles de seguridad en la plataforma tecnológica de la entidad	Sistemas	Controles implementados en la plataforma tecnológica	100%	1/2/2023	30/12/2023	20%
4	Ejecutar el plan de mejoramiento de la auditoría interna para la certificación en ISO 27001 del proceso de copias de seguridad	Sistemas	Seguimiento Plan de Mejoramiento	100%	1/1/2023	30/8/2023	40%

c. Plan tratamiento de riesgos de seguridad y privacidad de la información

En la cual se mantiene la actividad de implementación, monitoreo y seguimiento de la matriz de riesgos de seguridad digital, para la cual se han adelantado mesas de trabajo con la oficina de control interno, de manera que se tengan en cuenta aspectos de vulnerabilidad de los sistemas de Capital, eventos de pérdida de información e indisponibilidad que puedan afectar el correcto funcionamiento de la entidad.

Plan de actividades							
No.	Actividad a desarrollar	Responsable	Indicador y/o producto esperado	Meta programada	Cronograma		Ponderación
					INICIO	FIN	100%
1	Implementación, seguimiento y monitoreo de la matriz de riesgos de seguridad digital	Sistemas	Matriz de riesgos de seguridad digital	100%	1/2/2023	30/12/2023	100%

Respecto a lo indicado de manera previa se requiere que el área implemente mejoras respecto a:

- Relación del universo de los productos que permita medir el cumplimiento de estas, teniendo en cuenta lo formulado en los diferentes planes. Como ejemplo de lo anterior, el producto relacionado en la actividad 6 del Plan Estratégico de Tecnologías de la Información: Módulos administrativos implementados del ERP, así como del producto de la actividad 2: Funcionando los servicios.
- Determinar herramientas que permitan adelantar seguimiento de las actividades formuladas por parte del área, de manera que se realice un reporte coherente y debidamente soportado de los indicadores identificados.
- Revisar y fortalecer la herramienta de seguimiento a las actividades del plan de tecnologías de la información – PETI, de manera que se cuente con la información de lo ejecutado y que el reporte sea coherente con el porcentaje reportado en la matriz de monitoreo, ya que el promedio de ejecución para lo corrido de la vigencia 2023 se registra en 23,75% y la herramienta arroja un promedio de 24%, al establecerse el mismo porcentaje para todas las actividades formuladas.
- Realizar el monitoreo de la totalidad de las actividades, teniendo en cuenta que no es posible determinar el cumplimiento de estas sin el debido análisis de lo adelantado y el soporte correspondiente que dé cuenta de ello.
- Definir de manera clara y precisa las actividades a desarrollar dentro de los diferentes planes formulados, de manera que se puedan correlacionar los soportes entregados y el análisis correspondiente en los diferentes seguimientos que se adelantan en el canal. Como ejemplo de lo anterior: Actividad 2 del Plan Estratégico de Tecnologías de la Información: LDAP y GOOGLE y actividad 5: Actualización intranet.

- Revisar el documento de Indicadores de Gestión de Seguridad de la Información V4 del Ministerio de Tecnologías de la Información y las Comunicaciones con el fin de adoptar los indicadores que permitan medir el modelo que se viene implementando en Capital de manera adecuada.

11.9. GESTIÓN DOCUMENTAL DEL PROCESO

Teniendo en cuenta las recomendaciones generadas en el marco de la Circular 003 de 2023 del Archivo General de la Nación, se hace necesario que el área organice la información que se genera de la ejecución de sus actividades diarias, ya que las carpetas creadas en el repositorio habilitado por el área de gestión documental [https://drive.google.com/drive/folders/1M-R-snsXFSeQ26nQ1VMNA6-Ycl17nelC?usp=drive_link] para la vigencia 2022 se encuentra documentación sin encabezado, y se duplican los documentos publicados en la intranet, así mismo, para la vigencia 2023 se evidencia la existencia de carpetas vacías.

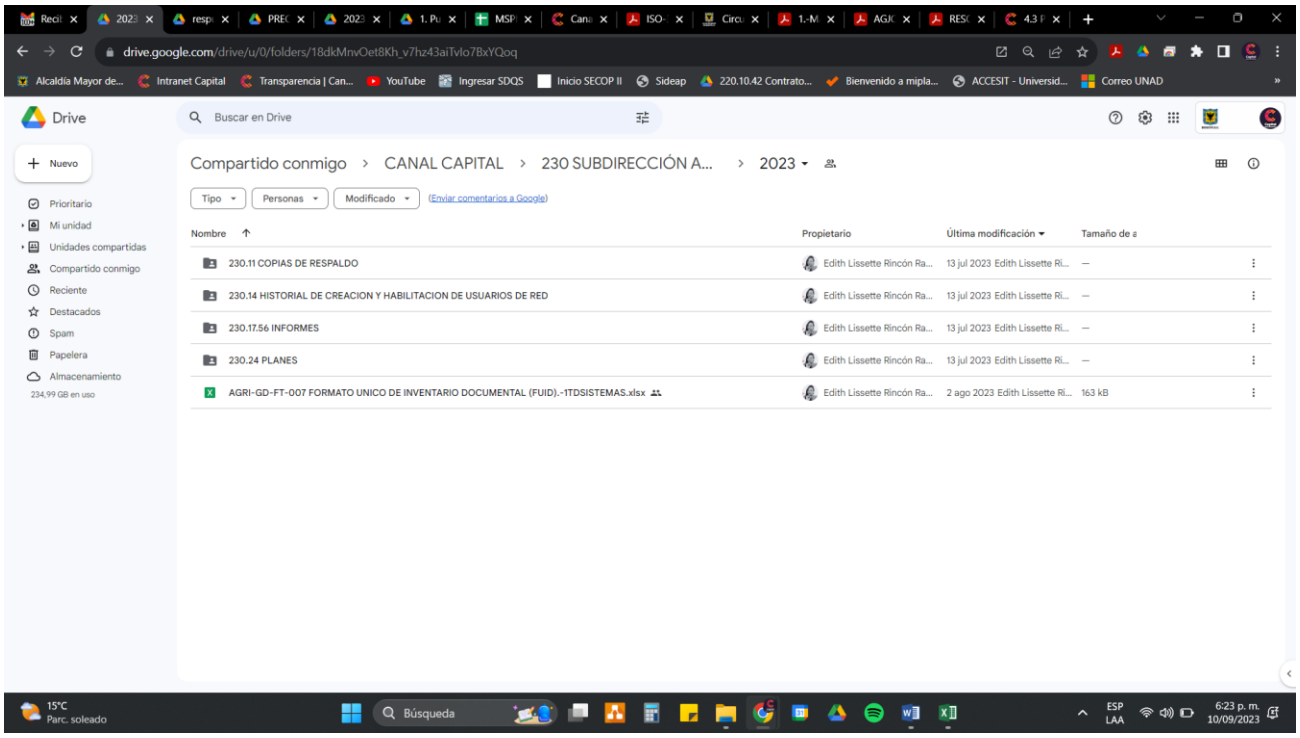
Backup Exec

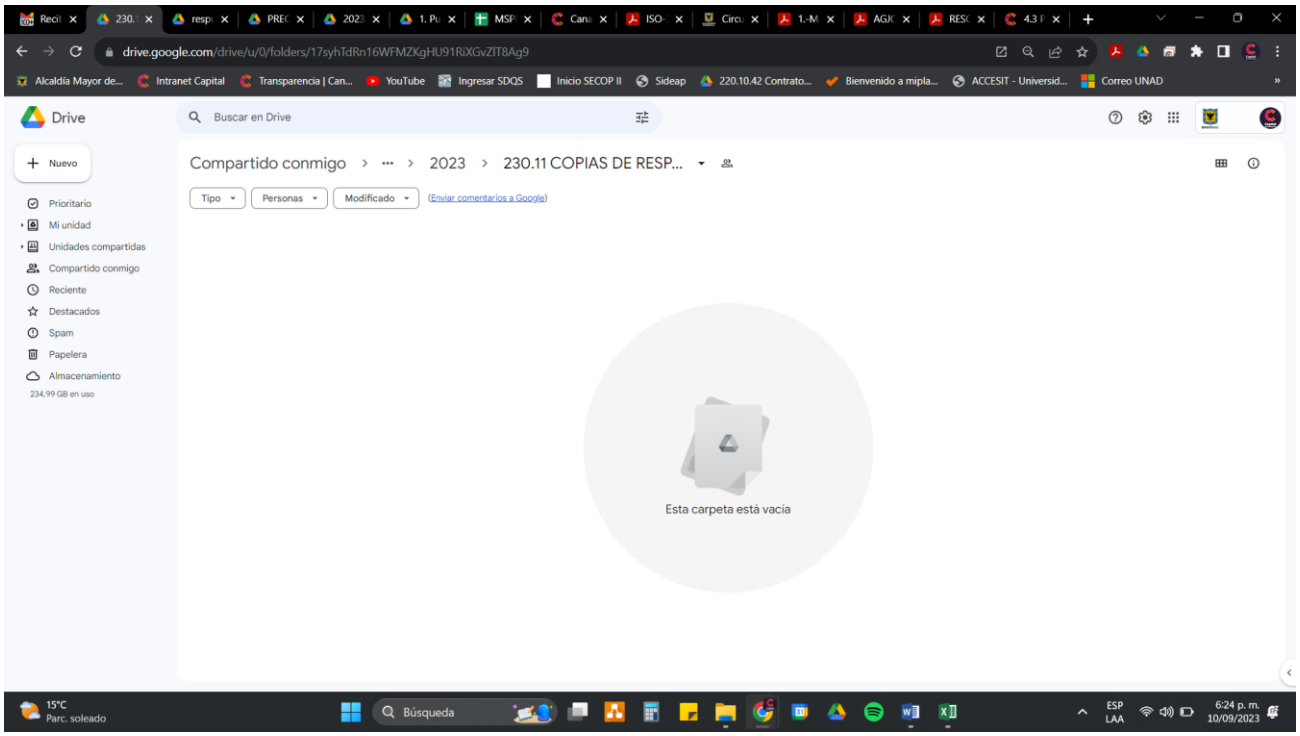
Numero de cintas

ORDEN	NUMERO DE CINTA	AÑO
346	CCA402L5	2022
347	CCA403L5	2022
348	CCA404L5	2022
349	CCA406L5	2022
350	CCA408L5	2022
351	CCA409L5	2022
352	CCA410L5	2022
353	CCA411L5	2022
354	CCA412L5	2022
355	CCA413L5	2022
356	CCA414L5	2022
357	CCA415L5	2022
358	CCA416L5	2022
359	CCA417L5	2022
360	CCA418L5	2022
361	CCA419L5	2022
362	CCA420L5	2022
363	CCA421L5	2022
364	CCA422L5	2022
365	CCA423L5	2022
366	CCA424L5	2022
367	CCA425L5	2022
368	CCA426L5	2022
369	CCA427L5	2022
370	CCA428L5	2022
371	CCA429L5	2022
372	CCA430L5	2022
373	CCA431L5	2022
374	CCA432L5	2022
375	CCA433L5	2022
376	CCA434L5	2022
377	CCA435L5	2022

Página 1 de 3

Fuente: Repositorio Sistemas, 2023.





Por último, si bien se adelanta el levantamiento del inventario documental del proceso, no es posible determinar que se cuente con la totalidad de la información generada en dicho documento, ya que, no es posible identificar la totalidad de documentos relacionados en la TRD del área, y por ende, mitigar una

pérdida de información al no contar con un sistema de control sobre el repositorio y ante la ausencia de un lineamiento interno sobre el tema [Información recolectada vía Google Forms].

Con lo anterior, se determina que no se da cabal cumplimiento a los principios de gestión documental definidos en la Política de gestión Documental [AGRI-GD-PO-001, versión 3 del 02 de noviembre de 2022] enmarcados en:

a. Control y seguimiento. Se debe asegurar el control y seguimiento de la totalidad de los documentos que produce o recibe en desarrollo de sus actividades, a lo largo de todo el ciclo de vida, es decir desde la planeación hasta la disposición final.

b. Oportunidad. Se deberán implementar mecanismos que garanticen que los documentos estén disponibles cuando se requieran y para las personas autorizadas para consultarlos y utilizarlos.

c. Disponibilidad. Los documentos deben estar disponibles cuando se requieran independientemente del medio de creación.

Así como lo definido en el Artículo 2.8.2.7.7. del Decreto 1080 de 2015, que señala: *"Requisitos para la disponibilidad de los documentos electrónicos de archivo. Los documentos electrónicos y la información en ellos contenida, debe estar disponible en cualquier momento, mientras la entidad está obligada a conservarla, de acuerdo con lo establecido en las Tablas de Retención Documental (TRD)".* **(Subrayado fuera de texto)** y de lo definido en la dimensión 5 del Manual operativo del Modelo Integrado de Planeación y Gestión – MIPG, versión 4 respecto a *"la interiorización de una cultura archivística por el posicionamiento de la gestión documental que aporta a la optimización de la eficiencia y desarrollo organizacional y cultural de la entidad y la comunidad de la cual hace parte, mediante la gestión del conocimiento, gestión del cambio, la participación ciudadana, la protección del medio ambiente y la difusión".*

11.10. ANÁLISIS DE RESPUESTAS SOBRE EL INFORME PRELIMINAR

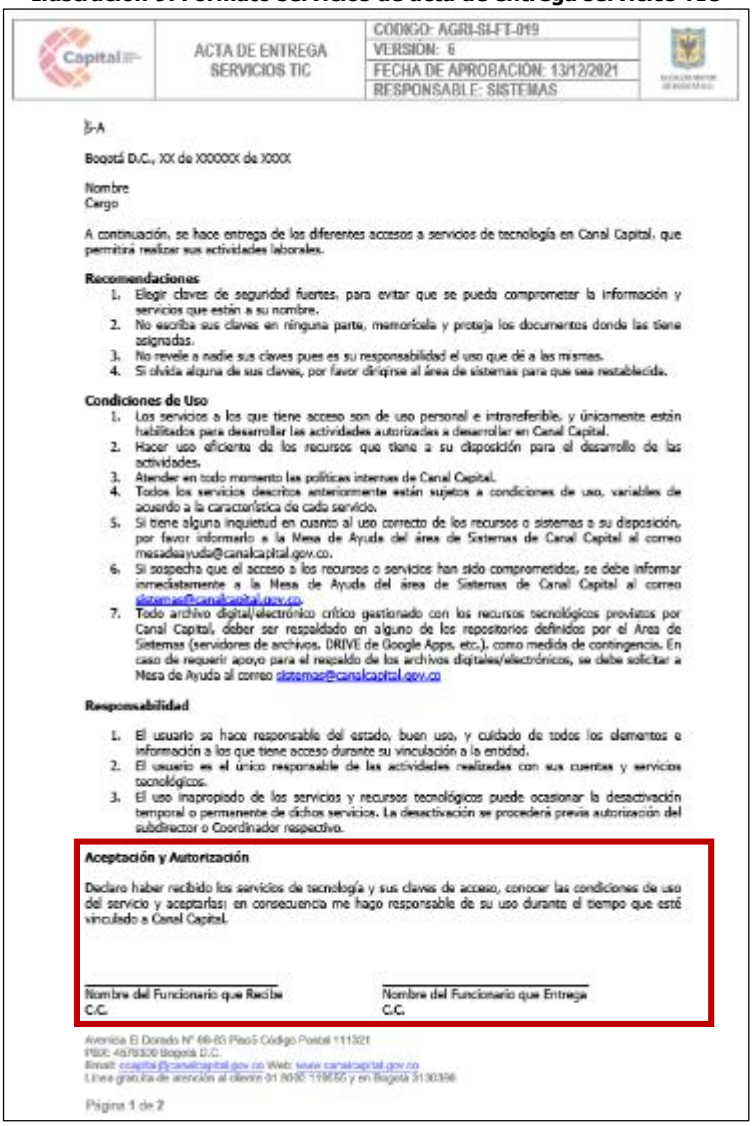
a. Teniendo en cuenta la respuesta remitida al informe preliminar de auditoría, recibida vía correo electrónico el 24 de octubre de 2023, así como la mesa de aclaración de dudas realizada el mismo día con el área de Sistemas, se consolida en la tabla 3 el análisis a cada comentario y soporte remitido por los responsables:

Tabla 3. Análisis respuesta informe preliminar

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
1	Control 5.2. Roles y responsabilidades de seguridad de la información	Se acepta parcialmente, ya que la Política fue actualizada y se hicieron ajustes en cuanto a los responsables.	Se remite la Política de Seguridad y privacidad de la información en su versión 6 del 09 de agosto de 2023, en la que se observan las mismas debilidades y otras adicionales frente a la asignación de compromisos de los responsables indicados en el numeral 7. Responsabilidades. Lo anterior para: **1.** Compromiso Comité Institucional de Gestión y Desempeño de Capital: Ítem 1, No es responsabilidad del CIGD actualizar y presentar la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información de conformidad con los lineamientos de la Política de administración del riesgo aprobada el 5 de diciembre de 2022. Ítem 3: La responsabilidad señalada en este ítem se indica que es para la Gerencia, "La Gerente y/o jefe de área es el responsable de hacer cumplir las normas y políticas de seguridad de la información establecidas por la Gerencia en Capital" por lo tanto, esta responsabilidad debe incluirse en el numeral 7.1 Compromiso de la Gerencia. **2.** Compromiso Oficina de Control Interno [ítem 1, teniendo en cuenta que las actividades deben ser concertadas con la Oficina de control interno, dado los requerimientos de conocimiento técnico requeridos para	x	

			realizar auditorías a los Sistemas de Información] **3.** Responsabilidades de los propietarios de la información [ítem 5, teniendo en cuenta que el área de Sistemas como líder de la Política es responsable de divulgar los requisitos indicados a las partes interesadas. Lo anterior, aplica de igual manera para el ítem 13 del numeral 7.6. Responsabilidades de los funcionarios, contratistas y terceros usuarios de la información.		
2	Control 5.17 Información de autenticación	Por políticas del servicio no se solicitan firmas, es enviado por correo electrónico, "Respetando la política de cero papel de la entidad solicitamos sea firmada o responder con un mensaje de aceptación". No se acepta, en la mayoría de activaciones, las solicitudes recibidas son para entrega de carné, ocasionalmente (caso periodistas y productores) les piden también usuario de Windows. Siguiendo el lineamiento de cero papel, pasados 3 días hábiles de recibida el acta, si no la devuelven firmada se da por aceptada y firmada.	Se remiten pantallazos de solicitud de servicios TIC 2022 - 2023 para (49) usuarios; sin embargo, no se remiten soportes de la remisión del acta para la firma correspondiente; así mismo, verificado el formato actualizado el 13 de diciembre de 2021 se evidencian los espacios para firmar como aceptación y autorización del uso de los servicios asignados. Teniendo en cuenta lo anterior, la recomendación de revisión y ajuste del formato se mantiene, de manera que se adapte con las condiciones mencionadas en la respuesta. [Ilustración 9. Formato servicios de acta de entrega servicios TICIlustración 9. Formato servicios de acta de entrega servicios TIC] De manera adicional en el Manual de gestión de usuarios, versión 2 del 13 de diciembre de 2021 no se indican los parámetros de aceptación mencionados por el área en la respuesta del informe preliminar, por lo que se debe adelantar el ajuste con el establecimiento de los términos, así como de las condiciones del formato. Teniendo en cuenta lo mencionado anteriormente.	x	

Ilustración 9. Formato servicios de acta de entrega servicios TIC



ACTA DE ENTREGA SERVICIOS TIC

CODIGO: AGRI-SI-FT-019
VERSIÓN: 6
FECHA DE APROBACIÓN: 13/12/2021
RESPONSABLE: SISTEMAS

5-A

Bogotá D.C., XX de XXXXX de XXXX

Nombre
Cargo

A continuación, se hace entrega de los diferentes accesos a servicios de tecnología en Canal Capital, que permitirá realizar sus actividades laborales.

Recomendaciones

1. Elegir claves de seguridad fuertes, para evitar que se pueda comprometer la información y servicios que están a su nombre.
2. No escriba sus claves en ninguna parte, memorícela y proteja los documentos donde las tiene asignadas.
3. No revele a nadie sus claves pues es su responsabilidad el uso que dé a las mismas.
4. Si olvida alguna de sus claves, por favor diríjase al área de sistemas para que sea restablecida.

Condiciones de Uso

1. Los servicios a los que tiene acceso son de uso personal e intransferible, y únicamente están habilitados para desarrollar las actividades autorizadas a desarrollar en Canal Capital.
2. Hacer uso eficiente de los recursos que tiene a su disposición para el desarrollo de las actividades.
3. Atender en todo momento las políticas internas de Canal Capital.
4. Todos los servicios descritos anteriormente están sujetos a condiciones de uso, variables de acuerdo a la característica de cada servicio.
5. Si tiene alguna inquietud en cuanto al uso correcto de los recursos o sistemas a su disposición, por favor informarlo a la Mesa de Ayuda del área de Sistemas de Canal Capital al correo mesadeayuda@canalcapital.gov.co.
6. Si sospecha que el acceso a los recursos o servicios han sido comprometidos, se debe informar inmediatamente a la Mesa de Ayuda del área de Sistemas de Canal Capital al correo sistemas@canalcapital.gov.co.
7. Todo archivo digital/electrónico crítico gestionado con los recursos tecnológicos provistos por Canal Capital, deber ser respaldado en alguno de los repositorios definidos por el Area de Sistemas (servidores de archivos, DRIVE de Google Apps, etc.), como medida de contingencia. En caso de requerir apoyo para el respaldo de los archivos digitales/electrónicos, se debe solicitar a Mesa de Ayuda al correo sistemas@canalcapital.gov.co

Responsabilidad

1. El usuario se hace responsable del estado, buen uso, y cuidado de todos los elementos e información a los que tiene acceso durante su vinculación a la entidad.
2. El usuario es el único responsable de las actividades realizadas con sus cuentas y servicios tecnológicos.
3. El uso inapropiado de los servicios y recursos tecnológicos puede ocasionar la desactivación temporal o permanente de dichos servicios. La desactivación se procederá previa autorización del subdirector o Coordinador respectivo.

Aceptación y Autorización

Declaro haber recibido los servicios de tecnología y sus claves de acceso, conocer las condiciones de uso del servicio y aceptarlas; en consecuencia me hago responsable de su uso durante el tiempo que esté vinculado a Canal Capital.

Nombre del Funcionario que Recibe
C.C.

Nombre del Funcionario que Entrega
C.C.

Avenida El Dorado Nº 66-63 Piso5 Código Postal 111321
PBX: 4378300 Bogotá D.C.
Email: ccapital@canalcapital.gov.co Web: www.canalcapital.gov.co
Línea gratuita de atención al ciudadano 01 8000 119055 y en Bogotá 3130356

Página 1 de 2

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
3	Control 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.	Ya se encuentra en un plan de mejoramiento y la guía de gestión de incidentes de seguridad de la información fue actualizada acorde a la guía del MINTIC.	Teniendo en cuenta que la guía de gestión de incidentes de seguridad de la información fue actualizada en Septiembre de 2022 en el marco del plan de mejoramiento por procesos vigente del área de Sistemas (por fuera del alcance de la presente auditoría), y los responsables indican que ya se incluyeron los elementos faltantes de conformidad con los lineamientos del MinTic este será evaluado en la próxima auditoría al modelo del MSPI. Se recomienda la socialización y capacitación de la guía actualizada a todos los colaboradores de la entidad.	x	
4	Control 5.25 Evaluación y decisión sobre eventos de seguridad de la información				

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
5	Control 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales	No se acepta, ya que para la vigencia del 2022 fue actualizado, y en la actual vigencia se encuentra en proceso de revisión y actualización de acuerdo a solicitud por parte del área de planeación.	Si bien se adelantó la actualización del normograma del área durante la vigencia 2022 con correo del 27 de enero de 2022 [como se indica en la respuesta], se reitera que se adelantó la verificación del normograma publicado por el área de Planeación en la intranet con fecha del 2023/01/06 en el cual no se incluye normatividad en materia de gobierno digital, seguridad de la información, por lo que, teniendo en cuenta que se viene realizando la revisión y actualización de dicho documento, se debe adelantar la verificación de la normatividad asociada faltante [de conformidad con la respuesta del área de Sistemas].	x	
6	Control 5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información	No se acepta, ya que el seguimiento a la implementación de las actividades del plan de seguridad y privacidad de la información se realiza a través del Plan de acción institucional y este se socializa ante el Comité por parte de Planeación.	Teniendo en cuenta que el control se enfoca en el liderazgo y establecimiento del compromiso de la organización respecto al Sistema de Seguridad de la Información mediante el establecimiento, cumplimiento de la Política de seguridad y privacidad de la información, comunicación y revisión periódica, no se observa en dicho documento que esta guarde relación con otros documentos con la que se dé cumplimiento a las responsabilidades; ejemplo, el plan de seguridad y privacidad de la información como se indica en la respuesta. Así mismo, como se indica en el numeral 11.5. del presente documento, es importante adelantar el monitoreo y seguimiento por parte del área de Sistemas respecto al esquema de actividades establecidas sobre las fases de implementación, evaluación y seguimiento de manera que sean coherentes con el reporte adelantado a los indicadores formulados [remitido dentro de los soportes de auditoría y respuesta al informe preliminar].	x	
7	Control 6.2 Términos y condiciones de empleo	No se acepta, ya que en las jornadas de inducción y reinducción se socializan aspectos del SGSI, así mismo, el área realiza capacitaciones en el marco de talento humano en temáticas de Seguridad y Ciberseguridad.	Se dio respuesta parcial a la debilidad detectada, ya que, se indica en el informe preliminar de auditoría que "no se evidencian las responsabilidades de la entidad en materia de seguridad de la información" en las minutas contractuales de la entidad. Frente a esto no se da respuesta en el informe. Frente a la falta de comunicación y socialización a los colaboradores de Capital sobre las responsabilidades que tienen frente a la seguridad de la información se adjuntan como soportes listados de asistencias a diferentes jornadas de capacitación realizadas por Sistemas, sin embargo, no hay soportes que permitan evidenciar los contenidos tratados en cada una de estas jornadas para determinar si se informó sobre esta temática en particular.	x	
8	Control 6.3 Concientización, educación y capacitación en seguridad de la información.	No se acepta, el plan ya fue actualizado para la vigencia actual.	Se remite por parte del área de Sistemas el Plan de seguridad y privacidad de la información, versión 2 del 21 de diciembre de 2022 en el cual se indican actividades de implementación y seguimiento para la vigencia 2023; sin embargo, no se observan dentro de las actividades mencionadas jornadas de capacitación, educación y concientización, así como tampoco se observa relación o coordinación de jornadas con el área de Recursos Humanos, al igual que un plan de trabajo o cronograma mediante los cuales se pueda monitorear la ejecución de estas. [Ilustración 10. Plan de seguridad y privacidad de la información]	x	

Ilustración 10. Plan de seguridad y privacidad de la información

Capital	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AGRI-SI-PL-003 VERSIÓN: 02 FECHA: 21/12/2022 RESPONSABLE: SISTEMAS	ALCALDÍA MAYOR DE BOGOTÁ D.C.

8. ACTIVIDADES A DESARROLLAR

A continuación, se presenta el esquema de actividades establecido por el Área de Sistemas:

FASE	ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FINALIZACIÓN
Implementación	Participar en las mesas de trabajo de la Alta Consejería Distrital para la articulación del Sistema de Gestión de Seguridad de la Información con respecto al plan de cumplimiento a nivel distrital	Profesional Seguridad Informática	02/01/2023	30/12/2023
	Documentar políticas, procedimientos, lineamientos, instructivos, entre otros. Relacionados con el MSPI y Gobierno Digital.	Profesional Seguridad Informática	02/01/2023	30/12/2023
	Implementar la matriz de seguridad digital de la entidad.	Profesional Seguridad Informática	02/01/2023	30/12/2023
	Actualizar el inventario de Activos de Información acorde a las Tablas de Retención Documental	Profesional Seguridad Informática	04/01/2023	30/12/2023
	Continuar con la implementación de la estrategia de comunicación del SGSI.	Profesional Seguridad Informática	03/01/2023	30/12/2023
	Implementar controles de seguridad en la plataforma tecnológica de la entidad	Profesional infraestructura y Seguridad Informática	02/01/2023	30/12/2023
Evaluación y Seguimiento	Implementar el plan de mejoramiento del SGSI.	Profesional Seguridad Informática	02/01/2023	30/12/2023

Página 13 de 13

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
9	Control 6.5 Responsabilidades después de la terminación o cambio de empleo.	No se acepta, la información que reposa en sus correos institucionales es responsabilidad de los mismos, de igual manera se restringe el acceso con el paz y salvo . (La entrega de material ligado a sus obligaciones contractuales, por lo tanto es tema de su supervisor).	Como se analiza en el informe, si bien Capital cuenta con la definición de las responsabilidades y deberes de seguridad de la información válidos para después de la terminación o cambio de empleo, no se observa la comunicación y/o divulgación de las responsabilidades de los usuarios de la información al interior de Capital. Teniendo en cuenta lo anterior, se mantiene la recomendación de aunar esfuerzos con las áreas, líderes de proceso y responsables del establecimiento de dichos parámetros para que comuniquen de manera oportuna y periódica la divulgación de estas. Teniendo en cuenta lo anterior, el soporte remitido del pantallazo de control de firma de paz y salvos no garantiza que se adelante la divulgación de las responsabilidades al término del contrato suscrito.	x	

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
10	Control 6.8 Informes de eventos de seguridad de la información	No se acepta, la guía de gestión de incidentes de seguridad de la información fue actualizada, de igual forma, en las diferentes charlas se mencionan los medios de comunicación de los posibles eventos.	Se dio respuesta parcial a la debilidad detectada, ya que, se indica en el informe preliminar de auditoría que "Para la vigencia 2022 se presentó un (1) incidente de seguridad: Anomalía o vulnerabilidad de software [15 de marzo de 2022], sobre el cual se determinaron acciones para atención del impacto; sin embargo, teniendo en cuenta la información suministrada durante la prueba no se registra la totalidad de actividades realizadas en equipos de la entidad y demás equipos" Frente a esto no se recibió respuesta. Teniendo en cuenta que la guía de gestión de incidentes de seguridad de la información fue actualizada en Septiembre de 2023 en el marco del plan de mejoramiento por procesos vigente del área de Sistemas (por fuera del alcance de la presente auditoría), y los responsables indican que ya se incluyeron los elementos faltantes de conformidad con los lineamientos del MinTic este será evaluado en la próxima auditoría al modelo del MSPI. Se recomienda la socialización y capacitación de la guía actualizada a todos los colaboradores de la entidad.	x	
11	Numeral 7.3.1 Etapa de Planeación - Documento Maestro del Modelo de Privacidad y Seguridad de la Información: Identificación de activos de información e infraestructura crítica.	No se acepta, el marco normativo no obliga establecer un procedimiento de activos de información, el canal cuenta con la GUÍA PARA EL INVENTARIO Y LA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN-AGRI-SI-GU-001, esta define la metodología para realizar la identificación y clasificación de los activos de información.	El MinTic emitió para las entidades obligadas a implementar el MSPI el Documento Maestro del Modelo de Seguridad y Privacidad de la Información: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf en el cual se establecen los lineamientos para "Proporcionar a las entidades mecanismos, lineamientos e instrumentos de implementación claros que les permitan adoptar, implementar y apropiar el MSPI con mayor facilidad", en este lineamiento no se indica que las entidades pueden determinar o escoger cuáles mecanismos e instrumentos implementar, las salidas indicadas en el documento se convierten en requisitos para la implementación del MSPI. Por lo anterior, en la fase planificación - numeral 7.3.1 Identificación de activos de información e infraestructura critica, se establece como salidas de esta etapa: Adoptar un Procedimiento de inventario y clasificación de la información y Documento metodológico de inventario y clasificación de la información. En la guía para el inventario y la clasificación de activos de información - AGRI -SI- GU -0001 se define la metodología utilizada por Capital para el levantamiento de los activos de información, sin embargo, falta el procedimiento indicado como salida.	x	
12	Numeral 7.3.3 Etapa de Planeación - Documento Maestro del Modelo de Privacidad y Seguridad de la Información: Identificación de activos de información e infraestructura crítica.	No se acepta, cuando se formuló el plan de tratamiento de riesgos fue aprobado en sesión 04 CIGD del 16-22/12/2020, para el proceso de actualización no es obligatorio realizar las aprobaciones por comité, ya que es dinámico de manera anual.	Cualquier documento que sea aprobado por el CIGD deberá ser llevado a esta misma instancia cada vez que se realicen actualizaciones o modificaciones del mismo. Como instancia que aprobó la primera versión del documento el CIGD debe estar al tanto de cualquier modificación del mismo pues es de su competencia evaluar y aprobar los cambios que se propongan, así como de realizar seguimiento al cumplimiento del mismo.	x	
13	Numeral 7.4.2 Etapa de Soporte - Competencia, toma de conciencia y comunicación.	Se adjunta archivo con la encuesta de satisfacción de servicios TI realizada.	Teniendo en cuenta que el soporte remitido no da cuenta de la implementación de la competencia, toma de conciencia y comunicación, de conformidad con el requisito normativo, se mantiene la calificación dada. [Ilustración 11. Soporte encuesta satisfacción]	x	

Ilustración 11. Soporte encuesta satisfacción

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
14	Control 7.8 Emplazamiento y protección de equipos	No se acepta, se realizan capacitaciones y se encuentran los lineamientos establecidos, siendo responsabilidad directa de los usuarios el uso adecuado de los recursos tecnológicos en el Manual de políticas se encuentra el siguiente lineamiento: "Los Colaboradores, Contratistas y Terceros que tengan a cargo estaciones de trabajo o equipos tecnológicos de propiedad de Capital deben bloquear estos en el momento de abandonar el puesto de trabajo con el fin	Si bien, en el manual de políticas complementarias se establece que es responsabilidad de los colaboradores, contratistas y terceros bloquear estos cuando se abandone el puesto de trabajo, en el control se establece que es necesario que los equipos se "puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña)" durante las pruebas de auditoría realizadas en las Sedes de la Calle 26 y Calle 69, se evidencio que para este control los usuarios pueden acceder a las configuraciones de los equipos modificar, eliminar o alargar los tiempos para que estos se bloqueen mediante un protector de pantalla protegido con contraseña, por lo cual se recomienda que sólo puedan acceder a las configuraciones de los equipos los responsables del área de Sistemas, y así evitar que se eliminen los bloqueos seguros.	x	

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
		de proteger el acceso indebido a la información en estos almacenada"			
15	Control 7.9 Seguridad de los activos fuera de las instalaciones	No se acepta. A y B) es incontrolable ya que es responsabilidad de cada usuario hacer buen uso y cuidado de los dispositivos asignados para realizar sus labores. C) A los usuarios en teletrabajo ya normalizados por Recursos Humanos, se les realizo verificación del puesto y equipo personal o corporativo para realizar Teletrabajo junto con las activación de VPN. A los colaboradores que se les asigna equipo, estos van alistados con Usuario Administrador Local y de Dominio, para impedir la modificación del sistema y protección del mismo, Antivirus y VVP realizar conexiones seguras con la oficina. D) Para el caso de cadena de custodia y de que colaborador o contratista hace uso de un dispositivo y que luego es trasferido a otro colaborador, para el Área de Sistemas es transparente, púes si bien en el formato de control de entrada y salida de equipos dice que quién hará uso, en la 2da casilla indica quien es el personal de planta o supervisor de contrato que se hace responsable del mismo y al cual se le trasfiere el equipo a su inventario de bienes, a los contratistas no se les asigna inventario. Posteriormente al finalizar el Cto la persona que tiene en uso un equipo, para solicitar su paz y salvo debe devolver el equipo a la oficina de Sistemas para tener su respectivo OK.	En el informe preliminar de auditoría se indicó que: Se debe complementar el manual de políticas complementarias *"**definiendo lineamientos que orienten a los colaboradores a ejecutar los siguientes criterios de seguridad de los activos fuera de las instalaciones"*** negrilla fuera de texto, de conformidad con este requisito, lo cual está acorde a la respuesta del área de Sistemas al informe preliminar donde se indica que *"A y B) es incontrolable ya que es responsabilidad de cada usuario hacer buen uso y cuidado de los dispositivos asignados para realizar sus labores"*, por lo indicado por el área es responsabilidad de la entidad indicar en el Manual de manera explícita la responsabilidad que tienen los colaboradores en este tema de conformidad como lo solicita el control. En el numeral C, lo que adicionalmente solicita el control es que se debe hacer una valoración de riesgos para controlar los lugares fuera de las instalaciones, tales como trabajo en casa, teletrabajo y sitios temporales y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina), esta valoración de riesgos no se encuentra documentada, se recomienda incluirla dentro de la matriz de riesgos de seguridad digital. En el numeral D, si bien a los contratistas de la entidad no se les asigna equipos sino a los supervisores y ellos son los responsables del mismo, lo que pide el control es que se lleve un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres de los responsables del equipo. Por lo anterior, se recomienda al área de Sistemas documentar un lineamiento en el que se establezca la responsabilidad frente al equipo y su información por parte de la persona autorizada a retirar y/o trasladar el equipo de las instalaciones del Canal.	x	

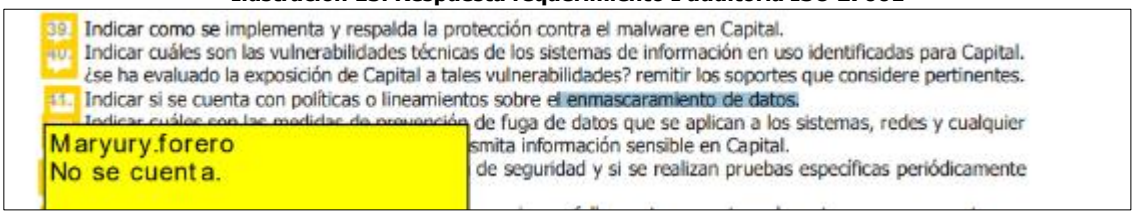
Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
16	Control 7.12 Seguridad del cableado	Se subsana lo que corresponde a sistemas, se le avisa a el área técnica lo que debe hacer en los espacios asignados a ellos ya que se pueden alterar los servicios.	Se evidencia que los cables del área de Gestión Documental fueron organizados en canaletas metálicas de conformidad con el requisito normativo, sin embargo, falta organizar el cableado correspondiente al área de tráfico. [Ilustración 12. Cableado área G. Documental] Se recomienda de manera articulada con SST realizar revisiones periódicas para evitar que se vuelvan a presentar situaciones similares y mitigar posibles accidentes.	x	

Ilustración 12. Cableado área G. Documental

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
23	Numeral 8.1 Etapa de Operación - Documento Maestro del Modelo de Privacidad y Seguridad de la Información: Planificación e implementación	No se acepta, la implementación de los controles se encuentra programados en el plan de seguridad de la información, de la siguiente forma: Implementar controles de seguridad en la plataforma tecnológica de la entidad.	En el plan de seguridad de la información se indica como una actividad: "Implementar controles de seguridad en la plataforma tecnológica de la entidad", en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información se establece como salida obligatoria de este numeral lo siguiente: Plan de implementación de controles de seguridad y privacidad de la información que contenga **como mínimo controles, actividades, fechas, responsable de implementación y presupuesto.** Negrilla fuera de texto. El plan de seguridad de la información falta desagregar los ítem señalados.	x	

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene? Si	No
17	Control 8.11	Las actividades de criptografía y enmascaramiento de datos son propias del desarrollo de software de la entidad y se encuentra conexo con la metodología de software y su arquitectura	Se remite pantallazo de los responsables ante la pregunta puntual que se realizó a través del memorando 459 de 2023, dónde se indica que no se cuenta con estas políticas. Verificado el documento indicado no hay lineamientos específicos frente al enmascaramiento de datos. [Ilustración 13. Respuesta requerimiento I auditoría ISO 27001]	x	

Ilustración 13. Respuesta requerimiento I auditoría ISO 27001



Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene? Si	No
18	Control 8.19 Instalación de software en sistemas operativos	No se acepta, la guía de alistamiento de equipos ya fue actualizada y publicada en la intranet.	Capital adelantó la construcción del documento "Guía de alistamiento de equipos de cómputo" en el que se adelanta la mención de pasos a tener en cuenta para instalación de software en equipos de cómputo en su versión 1; sin embargo, en atención al control establecido, si bien se establece que debe adelantarse por personal capacitado para tal fin, no se evidencia la definición de restricciones al usuario final que contemple instalaciones permitidas y los canales o medios de comunicación por medio de los cuales pueden ser requeridas, así como las prohibiciones (ejemplo, software personal) de la entidad. Teniendo en cuenta lo definido normativamente respecto al control: "Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios", se ajusta la calificación del control, pero se mantiene observación para que el área adelante los ajustes pertinentes.	x	
19	Control 8.23 Filtrado web	No se acepta, en la Política de seguridad de la información se encuentra inmersa la adaptación e implementación de las demás políticas en el manual.	Si bien Capital cuenta con la Política de seguridad y privacidad de la información, no se observa en el contenido de esta los requisitos para abordar la detección de software malicioso, las responsabilidades de cada parte involucrada, ni la articulación con la documentación de identificación y comunicación de incidentes de seguridad que permita identificar las acciones y los procedimientos definidos en Capital para identificar la recepción de software mal intencionado. De igual manera, teniendo en cuenta las debilidades indicadas en el documento de continuidad del negocio, se recomienda al área contemplar las actividades y equipos correspondientes para el tratamiento de este tipo de situaciones.	x	
20	Control 8.24 Uso de criptografía	Las actividades de criptografía y enmascaramiento de datos son propias del desarrollo de software de la entidad y se encuentra conexo con la	Se remite por parte del área el documento "Guía metodológica de desarrollo de software Intranet" el cual no se encuentra adoptada dentro del sistema de gestión de Capital, en el proceso de Sistemas; si bien al interior del documento se desarrollan aspectos de criptografía, es importante tener en cuenta que el área tenga en cuenta los requisitos normativos requeridos en la NTC ISO 27001 para el control correspondiente adoptando los siguientes aspectos:	x	

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
		metodología de software y su arquitectura.	* Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. * Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. * Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información. Teniendo en cuenta lo mencionado, la observación se mantiene con la calificación asignada.		
21	Numeral 9.1.1 Etapa de Evaluación del Desempeño - Documento Maestro del Modelo de Privacidad y Seguridad de la Información: Planificación e implementación	No se acepta, ya que se revisaron y definieron indicadores en el marco del Decreto 612 en la ejecución y seguimiento de los planes que están a cargo de Sistemas, estas son las herramientas establecidas institucionalmente para llevar a cabo el seguimiento de las actividades. El MinTIC, tiene un marco de referencia a través de todo el MSPI, las entidades lo adoptan acorde a sus capacidades y necesidades institucionales.	En el Documento Maestro del Modelo de Seguridad y Privacidad de la Información: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf se establece como salida obligatoria de este numeral lo siguiente: Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos. De conformidad con lo indicado en el informe preliminar de auditoría a la fecha no se ha elaborado y socializado el informe de conformidad con el lineamiento que contenga la evolución y medición de la efectividad de los controles definidos en el plan de tratamiento de riesgos, la respuesta remitida por los responsables no atiende a la oportunidad de mejora indicada en el informe.	x	
22	Control 9.1.2 Auditoría Interna: Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.	Se realizan auditorías externas al SGSI, internamente se debe articular con CI.	Se remite como soporte por parte del área un documento de socialización de resultados de auditoría de seguridad de la información en la cual no se pueden determinar las acciones de mejora u observaciones identificadas por el ejecutor *externo* [Kreston RM S.A.], así mismo, se indica que de conformidad con el requerimiento las auditorías a realizar son **internas** por lo que no se realizan ajustes respecto a la calificación y observación identificada.	x	
23	Control 9.1.3 Revisión por la dirección: Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.	Ya hace parte del plan de mejoramiento vigente. Se realizó solicitud a Planeación para que de manera anual se realice seguimiento de ejecución del SGSI por parte del Comité. No es obligatorio aprobar manuales, los Planes y Política cuentan con dicha aprobación.	Se identifica dentro del plan de mejoramiento de la vigencia anterior una acción de mejora determinada "Gestionar con el Área de Planeación la periodicidad del seguimiento a la implementación del SGSI por parte del Comité de Gestión y Desempeño" con lo que se espera realizar la revisión por parte de la alta dirección a los temas de seguridad y privacidad de la información de Capital; sin embargo, respecto a la aprobación de los documentos se reitera que *"Todos los documentos del MSPI* ***deberán ser aprobados****, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad"*, Negrilla fuera de texto, teniendo en cuenta que este debe ser por parte de la alta dirección (Comité Institucional de Gestión y Desempeño). (Documento Maestro del Modelo de Seguridad y Privacidad de la Información, 2021).	x	

Ítem	Aspecto evaluado	Respuesta área	Análisis Oficina de control interno	¿Se mantiene?	
				Si	No
24	Numeral 10.1 Mejoramiento continuo - Documento Maestro del Modelo de Privacidad y Seguridad de la Información: Planificación e implementación	La implementación de los controles del MSPI, se espera que de manera anual el porcentaje de avance vaya incrementado de manera paulatina. por esa razón no se generan planes de mejoramiento, porque no se está incumpliendo la Norma, y para alcanzar el nivel óptimo es necesario incluir recursos y elementos que no es decisión directa del área de sistemas.	En el Documento Maestro del Modelo de Seguridad y Privacidad de la Información: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf se establece como salida obligatoria de este numeral lo siguiente: Plan anual de mejora del MSPI. Se reitera que si bien el área en sus ejercicios de autoevaluación no ha detectado incumplimientos o hallazgos, el MSPI no está implementado en un 100% en Capital, por lo cual para aquellos controles pendientes de implementar y los que son susceptibles de mejora de conformidad con el requisito normativo debe establecerse un plan anual de mejora. El proceso debe tener en cuenta que parte de este requisito de cumplirá con el plan de mejora que se derive del presente trabajo de auditoría, sin embargo, en sus ejercicios de autoevaluación deben establecerse acciones adicionales que permitan cerrar la brecha entre el 85% y lo que le falta a la entidad para cumplir la meta de la implementación total del modelo.	X	

b. Se indica por parte del área de Planeación, respecto al literal b del numeral 11.7 Riesgos:

> *Las amenazas de tipo ambiental están asociadas con aspectos de infraestructura que pueda verse vulnerada por fenómenos climáticos, inundaciones, sismos, incendios por condiciones naturales y factores meteorológicos, si bien es un tema que involucra la temática ambiental, son factores que se asocian más a actuaciones frente a emergencias derivadas de dichas amenazas, por ende, considero que este tema debe ligarse a SST y no a PIGA. Esto también teniendo en cuenta el capítulo 3.2. del Plan Institucional de Gestión Ambiental de la entidad.*

Sin embargo, en el marco de la auditoría no se indica que la responsabilidad de identificación de este tipo de riesgos deba adelantarse dentro de las actividades del Plan Institucional de Gestión Ambiental - PIGA o por el profesional de Seguridad y Salud en el Trabajo en el marco del SST. Lo anterior, deberá ser liderado por el área de Sistemas dentro de la implementación del Sistema de seguridad y privacidad de la información y articular a las áreas y procesos que se consideren pertinentes y que puedan apoyar dicha identificación.

12. OBSERVACIONES

N°	OBSERVACIONES
11.2	**DESCRIPCIÓN:** Debilidades en el diligenciamiento del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información, respecto al reporte de información incompleta al no indicar la brecha o aspectos a mejorar por parte de la entidad, porcentaje de cumplimiento alto sin la debida justificación, calificación de aspectos que no cumplen con los requisitos con altos porcentajes de cumplimiento. De conformidad con lo indicado en el numeral 11.2 **CRITERIO DE AUDITORÍA:** • Herramienta de autodiagnóstico del MSPI (Análisis GAP) • Documento maestro del Modelo de Privacidad y Seguridad de la Información – octubre de 2021.
11.3	**DESCRIPCIÓN:** Debilidades en la implementación de los lineamientos descritos en el documento maestro del Modelo de Privacidad y Seguridad de la Información, respecto a las fases de diagnóstico, planificación, operación, evaluación del desempeño y mejora continua, descritos de manera detallada en el numeral 11.3: **1.** No se evidencia en la política de Planeación Institucional la inclusión de aspectos como el modelo de procesos y servicios, así como necesidades y expectativas de las partes interesadas en materia del MSPI.

N°	OBSERVACIONES
	2. En el manual del MIPG de Capital no se evidencia la definición del alcance del MSPI. **3.** No se evidencia acto administrativo que adopte la Política de seguridad y privacidad de la información. Adicionalmente, en esta no se definen roles y responsabilidades en materia de ciberseguridad y T.I. **4.** No se cuenta con un procedimiento y documento metodológico de inventario y clasificación de información e infraestructura crítica. **5.** No se evidencia aprobación del CIGD del Plan de tratamiento de los riesgos de seguridad de la información. **6.** Establecer en las minutas de los contratos la responsabilidad que tiene Capital frente al cumplimiento de los temas relacionados con la seguridad de la información. **7.** Implementar herramientas de seguimiento para el Plan de cambio, cultura, apropiación, capacitación y sensibilización de seguridad y privacidad de la información. **8.** Definir un plan de implementación de controles de seguridad y privacidad de la información que contemple los requisitos mínimos normativos. **9.** Elaborar los informes con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos **10.** Para la vigencia 2022 no se realizaron auditorías al MSPI. **11.** No se cuentan con actas y/o soportes que permitan evidenciar la revisión por la Alta dirección de la política de seguridad y privacidad de la información. **12.** Establecer acciones de mejora para llevar al modelo al nivel de madurez optimizado. **CRITERIO DE AUDITORÍA:** ● Documento maestro del Modelo de Privacidad y Seguridad de la Información – octubre de 2021.
11.4.1	**DESCRIPCIÓN:** Debilidades [oportunidades de mejora] en la implementación de los controles definidos en la norma ISO 27001:2013, en los siguientes aspectos descritos de manera detallada en el numeral 11.4 y calificados con nivel de cumplimiento (2): **1.** Controles sobre política de seguridad de la información [A.5.1]. **2.** Controles sobre organización de seguridad de la información [A.6.1.1 - A.6.1.2 - A.6.1.5 - A.6.2.2] **3.** Controles de seguridad de los recursos humanos [A.7.1.2 – A.7.3.1.] **4.** Controles de gestión de activos [A.8.1.1 - A.8.2.1 - A.8.1.3] **5.** Controles sobre cumplimiento [A.18.1.1] **6.** Controles respecto a relaciones con los proveedores [A.15.1 – A.15.2] **7.** Controles sobre control de acceso [A.9.2.3 – A.9.2.4] **8.** Controles sobre seguridad física y del entorno [A.11.1.1 – A.11.2.1 – A.11.2.9 – A.11.2.8 – A.11.2.6 – A.11.2.3, A.11.2.7] **9.** Controles sobre seguridad de las operaciones [A.12.6 – A.12.6.2] **10.** Controles de seguridad de las comunicaciones [A.13.2] **11.** Controles sobre adquisición, desarrollo y mantenimiento de sistemas [A.14.2.1 – A.14.25 – A.14.2.7] **12.** Controles sobre incidentes de seguridad de la información [A.16.1.1] **CRITERIO DE AUDITORÍA:** ● Política de privacidad y seguridad de información AGRI-SI-PO-001 – V1 ● Política de Administración de Riesgos de Capital EPLE-PO-001 – V8 ● Manual Metodológico para la Administración de Riesgos de Capital EPLE-MN-003 – V5 ● Procedimientos de transferencias primarias AGRI-GD-PD-001 -V10 ● Procedimiento de transferencias secundarias AGRI-GD-PD-002 – V9 ● Manual de Gestión de Usuarios AGRI-SI-MN-005 – V2 ● Actas de entrega de servicios TIC AGRI-SI-FT-019 ● Guía de reporte de incidentes de seguridad AGRI-SI-GU-007 -V2

N°	OBSERVACIONES
	• Plan de sensibilización del sistema de gestión de seguridad y privacidad de la información AGRI-SI-PL-005 • Inventario de activos de información. • TRD del área de Sistemas. • Minutas contractuales. • Manual de políticas complementarias AGRI-SI-MN-006 – V3 • Matriz CMDB de inventarios AGRI-SI-FT-038 • Manual Técnico de despliegue de implementación de software AGRI-SI-MN-008 – V1 • NTC ISO 27001:2013
11.4.2	**DESCRIPCIÓN:** Falta de implementación de los siguientes controles definidos en la norma ISO 27001:2013 y descritos de manera detallada en el numeral 11.4, calificados con nivel de cumplimiento (1): **1.** Controles sobre política de seguridad de la información [A.5.1, A.5.2]. **2.** Controles sobre organización de seguridad de la información [A.6.1.5] **3.** Controles de seguridad de los recursos humanos [A.7.2.2] **4.** Controles sobre aspectos de seguridad de la información / de la gestión de la continuidad del negocio [A.17.1 – A.17.2 – A.17.3] **5.** Controles sobre control de acceso [A.9.2.2 – A.9.2.3 - A.9.2.4 - A.9.4.5 - A.9.1.1 - A.9.1.2] **6.** Controles sobre criptografía [A.10.1.1 – A.10.1.2] **7.** Controles sobre seguridad física y del entorno [A.11.2.5] **8.** Controles sobre seguridad de las operaciones [A.12.1.3 – A.12.3.1 – A.12.4.4 – A.12.7-A.12.2.1] **9.** Controles sobre incidentes de seguridad de la información [A.16.1.2 – A.16.1.4 – A.16.1.5 – A.16.1.6 – A.16.1.7] **CRITERIO DE AUDITORÍA:** • Política de privacidad y seguridad de información AGRI-SI-PO-001 – V1 • Política de Administración de Riesgos de Capital EPLE-PO-001 – V8 • Manual Metodológico para la Administración de Riesgos de Capital EPLE-MN-003 – V5 • Procedimientos de transferencias primarias AGRI-GD-PD-001 -V10 • Procedimiento de transferencias secundarias AGRI-GD-PD-002 – V9 • Manual de Gestión de Usuarios AGRI-SI-MN-005 – V2 • Actas de entrega de servicios TIC AGRI-SI-FT-019 • Guía de reporte de incidentes de seguridad AGRI-SI-GU-007 -V2 • Plan de sensibilización del sistema de gestión de seguridad y privacidad de la información AGRI-SI-PL-005 • Inventario de activos de información. • TRD del área de Sistemas. • Minutas contractuales. • Manual de políticas complementarias AGRI-SI-MN-006 – V3 • Matriz CMDB de inventarios AGRI-SI-FT-038 • Manual Técnico de despliegue de implementación de software AGRI-SI-MN-008 – V1 • NTC ISO 27001:2013
11.5	**DESCRIPCIÓN:** Debilidades en la documentación del proceso de Sistemas relacionados con el sistema de seguridad y privacidad de la información; sobre estos se hace necesaria la revisión y modificación, de manera que se mencionan las actividades que se adelantan al interior de Capital, y se actualicen y complementen de conformidad con las necesidades identificadas. Se describe de manera detallada para cada documento en el numeral 11.5: **1.** Manual del sistema de gestión de seguridad de la información-SGSI AGRI-SI-MN-001 V2

N°	OBSERVACIONES
	2. Manual de políticas complementarias AGRI-SI-MN-006 V3 **3.** Guía de borrado seguro de información AGRI-SI-PD-014 V10 **4.** Plan de continuidad del NEGOCIO AGRI-SI-PL-002 V1 **5.** Gestión de cambios de tecnologías de la información AGRI-SI-PD-020 V1 **6.** Manual de gestión de USUARIOS AGRI-SI-MN-005 V2 **7.** Plan de seguridad y privacidad de la información AGRI-SI-PL-003 V2 **8.** Plan de tratamiento de riesgos de seguridad y privacidad de la información AGRI-SIPL-004 V3 **9.** Plan de sensibilización del sistema de gestión de seguridad y privacidad de la información agri-si-pl-005 V2 **CRITERIO DE AUDITORÍA:** • NTC ISO 27001:2013
11.6	**DESCRIPCIÓN:** Debilidades identificadas en el Plan Estratégico de las Tecnologías de Información PETI - AGRI-SI-PL-001, respecto a la falta de actualización del documento y a la falta de herramienta(s) de seguimiento adecuada(s) que permita(n) determinar el nivel de cumplimiento tanto físico como presupuestal de cada uno de los proyectos del PETI, y que permitan soportar el porcentaje de cumplimiento reportado en los proyectos de inversión. Así como su debida socialización y aprobación por parte del CIGD. Lo anterior se describe de manera detallada en el numeral 11.6. **CRITERIO DE AUDITORÍA:** • Plan Estratégico de las Tecnologías de Información PETI - AGRI-SI-PL-001. • Hoja de ruta de PETI – 2023
11.6.1	**DESCRIPCIÓN:** Debilidades en las actividades de integración y publicación de planes requeridos en el Decreto 612 de 2018, respecto a: **1.** Falta la publicación e integración del Plan Estratégico de las Tecnologías de la Información formulado para la vigencia 2023 al plan de acción institucional de Capital. **2.** Capital no incluyó en la guía: LINEAMIENTOS PARA PUBLICACIÓN DE INFORMACIÓN EN LA SEDE ELECTRÓNICA – V5 un lineamiento que indique que se debe realizar la publicación del PETI por parte de los responsables antes del 31 de enero de la vigencia, ni se cuenta con un espacio en el botón de transparencia para hacer la publicación e integración de los planes indicados en del Decreto 612 de 2018. Lo anterior se describe de manera detallada en el numeral 11.6.1 **CRITERIO DE AUDITORÍA:** • Decreto 612 de 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado" • LINEAMIENTOS PARA PUBLICACIÓN DE INFORMACIÓN EN LA SEDE ELECTRÓNICA – V5
11.7	**DESCRIPCIÓN:** Debilidades en la matriz de riesgos e identificación de riesgos de seguridad digital respecto a: **1.** No se valoran los riesgos (probabilidad e impacto) con la escala establecida en Política de Administración de Riesgos de Capital EPLE-PO, ya que, no se estableció una escala diferencial para los riesgos de seguridad digital. **2.** Se deben identificar riesgos e implementar controles contra amenazas de tipo ambiental. **3.** Se deben identificar riesgos e implementar controles para garantizar la seguridad de los activos fuera de las instalaciones de Capital que pueden contener información sensible

N°	OBSERVACIONES
	de la entidad, para aquellos colaboradores que ejerzan su función en la modalidad de teletrabajo, trabajo remoto o lugares temporales dada la misionalidad de Capital. Lo anterior se describe de manera detallada en el numeral 11.7 **CRITERIO DE AUDITORÍA:** • Política de Administración de Riesgos de Capital EPLE-PO-001 – V8 • Manual Metodológico para la Administración de Riesgos de Capital EPLE-MN-003 – V5 • Matriz de riesgos de seguridad digital V1 y V2 • ISO 27001:2013
11.8	**DESCRIPCIÓN:** Debilidades en el reporte de los indicadores identificados al interior del área, teniendo en cuenta: **1.** Falta la relación del universo de actividades que permita medir el cumplimiento de las actividades formuladas en los diferentes planes. **2.** Determinar herramientas que permitan adelantar seguimiento de las actividades formuladas por parte del área, de manera que se adelante un reporte coherente y debidamente soportado de los indicadores identificados. **3.** Revisar y fortalecer la herramienta de seguimiento a las actividades del plan de tecnologías de la información – PETI, de manera que se cuente con la información de lo ejecutado y que el reporte sea coherente con el porcentaje reportado en la matriz de monitoreo. **4.** Realizar el monitoreo de la totalidad de las actividades, teniendo en cuenta que no es posible determinar el cumplimiento de estas sin el debido análisis de lo adelantado y el soporte correspondiente que dé cuenta de ello. **5.** No se evidencia la adopción de algunos de los indicadores propuestos en el documento: Indicadores de Gestión de Seguridad de la Información V4 Lo anterior se describe de manera detallada en el numeral 11.8 **CRITERIO DE AUDITORÍA:** • Plan de acción institucional 2022 y 2023. • Manual del sistema de medición y seguimiento V2 • Manual Operativo MIPG V5 • Indicadores de Gestión de Seguridad de la Información V4
11.9	**DESCRIPCIÓN:** Debilidades frente al cumplimiento de los principios de gestión documental respecto al control y seguimiento, oportunidad y disponibilidad de la información del área, ya que las carpetas creadas se encuentran vacías e información que no cuenta con encabezados que permitan identificar con facilidad el contenido de la información. Lo anterior se describe de manera detallada en el numeral 11.9 **CRITERIO DE AUDITORÍA:** • GUÍA DE LINEAMIENTOS PARA EL USO Y ALMACENAMIENTO DE DOCUMENTOS DIGITALES Y/O ELECTRÓNICOS EN CANAL CAPITAL. • TRD del área de Sistemas. • Decreto 1080 de 2015 *"Por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura"*
10	**TOTAL**

13. CONCLUSIONES

Se da cumplimiento al objetivo formulado en la auditoría de verificar el nivel de ejecución de los lineamientos establecidos en la norma ISO 27001, sobre lo cual se resaltan aspectos como:

13.1. El área de Sistemas adelantó la autoevaluación del Modelo de Seguridad y Privacidad de la Información en la herramienta determinada por MinTic.

13.2. Se cuenta con la conformación del Comité de Gestión y Desempeño mediante acto administrativo 081 de 2021 por la cual se organiza el Modelo Integrado de Planeación y Gestión de Capital, en el cual se asignan responsabilidades frente a la seguridad digital.

13.3. Capital durante el periodo evaluado implementó y actualizó lineamientos: Guías, manuales y planes requeridos para la implementación y mejora del Modelo de seguridad y Privacidad de la Información - MSPI.

13.4. Se cuenta con la definición del plan estratégico de tecnologías de la información – PETI para el periodo 2021-2024.

13.5. Se adelantó el ejercicio de identificación de riesgos de seguridad digital para Capital y la matriz se actualizó a su versión 2.

13.6. Se adelanta la verificación de los antecedentes de los colaboradores previo a la vinculación de estos a la entidad de manera general, sin importar la información a la que se tiene acceso en el marco de la ejecución de sus obligaciones.

13.7. Se ha mejorado el respaldo eléctrico antes cortes de energía en las Sedes de la Calle 26 y la Casa de la 69.

13.8. Se ha promovido el desarrollo de software in-house, para atender las necesidades específicas de las diferentes áreas de Capital, y se han establecido entornos separados de pruebas y producción para el desarrollo de software.

13.9. Se evidencia la asignación de recursos financieros y humanos a través del proyecto de inversión 7511"Fortalecimiento de la capacidad administrativa y tecnológica para la gestión institucional de Capital" de Capital, para implementar y mejorar el modelo MSPI.

De igual manera, se presentan oportunidades de mejora respecto a:

13.10. Se deben complementar los lineamientos de Capital en materia de MSPI de conformidad con los requisitos mínimos establecidos en el documento maestro del Modelo de Seguridad y Privacidad de la Información del MinTic y sus guías de orientación.

13.11. Se requiere que el área adelante la revisión y modificación del reporte de información de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la vigencia, ya que, se reporta información incompleta, no se justifica adecuadamente los ítems que no aplican a Capital y se encuentran ítems calificados con altos porcentajes de avance que no se encuentran debidamente justificados.

13.12. Se evidencian debilidades en el acompañamiento, reporte y relación de avances en la ejecución de las actividades relacionadas con los indicadores que permiten medir el proceso de seguridad y privacidad de la información. De igual manera, se deben formular indicadores aplicables a Capital de conformidad con lo definido en el documento de indicadores de Gestión de seguridad de la información V4 del MinTic.

13.13. Para el periodo evaluado se actualizó la Hoja de ruta del PETI, pero no se actualizó paralelamente el documento denominado Plan Estratégico de las Tecnologías de Información PETI - AGRI-SI-PL-001,

adicionalmente no se publicó el PETI de Capital, antes del 31 de enero de las vigencias 2022 y 2023 en el botón de transparencia de conformidad con el Decreto 612 de 2018.

13.14. No se cuenta con una herramienta de seguimiento adecuada que permita evidenciar y soportar documentalmente el avance físico y presupuestal de las metas 3 y 4 del proyecto de inversión 7511 - Fortalecimiento de la capacidad administrativa y tecnológica para la gestión institucional de Capital.

13.15. Capital no incluyó en la guía: LINEAMIENTOS PARA PUBLICACIÓN DE INFORMACIÓN EN LA SEDE ELECTRÓNICA – V5 un lineamiento que indique cómo debe realizarse la publicación e integración en el botón de transparencia de los planes indicados en del Decreto 612 de 2018.

13.16. Se presentan debilidades respecto a la identificación de riesgos de seguridad digital, teniendo en cuenta que estos no contemplan la totalidad de actividades indicadas en el numeral 11.7. del presente informe, ni los criterios de evaluación de probabilidad e impacto se acogen a lo establecido en la Política de Administración de Riesgos de Capital EPLE-PO-001.

13.17. Se presentan debilidades respecto a la gestión documental del proceso al incumplir los principios definidos en la Política de gestión Documental respecto a la disponibilidad, oportunidad y control y seguimiento de la información generada por parte del proceso.

13.18. Se identifican debilidades en materia de la implementación de los controles establecidos en la norma ISO 27001:2013 en Capital, los cuales se calificaron como inexistentes o implementados, pero con debilidades u oportunidades de mejora.

13.19. Capital cuenta con Guía de Borrado Seguro de Información V2, donde se definen los lineamientos adoptados por la entidad para borrar de forma segura la información, sin embargo, se recomienda definir en la guía quién ejercerá la responsabilidad final de verificar que la información se haya eliminado segura y definitivamente, ya que no se establece ese punto de control.

13.20. El área de Sistemas define el uso de programas de utilidad que permiten el control de acceso a la información, a través del directorio activo mediante el cual se establecen las reglas de uso de la información de la entidad, sin embargo, deben fortalecerse los reportes que se hacen desde el área de Recursos Humanos en situaciones como incapacidades, vacaciones y encargos.

13.21. El documento de continuidad del negocio debe revisarse los elementos de alcance, referencias normativas aplicables, términos y condiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora, de manera que refleje la realidad de la entidad en materia de seguridad y privacidad de la información, entre otras actividades adelantadas por el área de Sistemas. Lo anterior, de conformidad con lo indicado en el numeral 11.5. del presente informe.

14. RECOMENDACIONES

14.1. Revisar y modificar la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información de la vigencia, de manera que esta cuente con información completa frente a la justificación de la calificación asignada para Capital.

14.2. Complementar los lineamientos de Capital en materia de MSPI de conformidad con los requisitos mínimos establecidos en el documento maestro del Modelo de Seguridad y Privacidad de la Información del MinTic y sus guías de orientación.

14.3. Fortalecimiento de las actividades de acompañamiento, reporte y relación de avances en la ejecución de las actividades relacionadas con los indicadores que permiten medir el proceso de seguridad y privacidad de la información.

14.4. Formular indicadores aplicables a Capital de conformidad con lo definido en el documento de indicadores de Gestión de seguridad de la información V4 del MinTic.

14.5. Actualizar de manera paralela el Plan Estratégico de las Tecnologías de Información PETI - AGRI-SI-PL-001, así como la hoja de ruta asociada y presentar al Comité de gestión y Desempeño.

14.6. Elaborar una herramienta de seguimiento adecuada que permita evidenciar y soportar documentalmente el avance físico y presupuestal de las metas 3 y 4 del proyectos de inversión 7511 - Fortalecimiento de la capacidad administrativa y tecnológica para la gestión institucional de Capital.

14.7. Incluir en la guía de LINEAMIENTOS PARA PUBLICACIÓN DE INFORMACIÓN EN LA SEDE ELECTRÓNICA – V5 un lineamiento que indique cómo debe realizarse la publicación e integración en el botón de transparencia de los planes indicados en del Decreto 612 de 2018.

14.8. Fortalecer la identificación de riesgos de seguridad digital, teniendo en cuenta que estos no contemplan la totalidad de actividades indicadas como son los criterios de evaluación de probabilidad e impacto y la escala de calificación, de manera que se acojan a lo establecido en la Política de Administración de Riesgos de Capital EPLE-PO-001.

14.9. Adelantar la identificación de riesgos y controles contra amenazas físicas y ambientales para minimizar el riesgo de afectaciones en la privacidad y seguridad de la información.

14.10. Fortalecer el proceso de gestión documental del área al incumplir los principios definidos en la Política de gestión Documental respecto a la disponibilidad, oportunidad y control y seguimiento de la información generada.

14.11. Fortalecer la implementación, monitoreo y demás actividades asociadas en materia de cumplimiento de lineamientos de la norma ISO 27001 en Capital, clasificados como inexistentes y definidos [con debilidades] en el proceso de auditoría.

14.12. Definir en la guía de Borrado Seguro de Información V2, quién ejercerá la responsabilidad final de verificar que la información se haya eliminado segura y definitivamente, ya que no se establece ese punto de control.

14.13. Fortalecer los reportes que se hacen desde el área de Recursos Humanos en situaciones como incapacidades, vacaciones y encargos al área de Sistemas con el fin de mantener las reglas de uso de la información de la entidad pertinentes a cada caso.

14.14. Actualizar el documento de Continuidad del negocio, de manera que se incluyan los elementos de alcance, referencias normativas aplicables, términos y condiciones, contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora, de manera que refleje la realidad de la entidad en materia de seguridad y privacidad de la información, entre otras actividades adelantadas por el área de Sistemas.

14.15. Poner a consideración las políticas del sistema de seguridad y privacidad de la información a las partes interesadas de manera que se reciban los comentarios y retroalimentaciones necesarias, de manera previa a la presentación en el Comité de gestión y desempeño del canal.

14.16. Elaborar una herramienta de comunicación de incidentes que le permita a los colaboradores de la entidad poner en conocimiento los incidentes en materia de seguridad para tratamiento por parte del área de Sistemas. De igual manera, adelantar la comunicación y socialización de esta al interior de Capital.

14.17. Adelantar capacitaciones y/o socializaciones relacionadas con los lineamientos emitidos por el área de Sistemas en materia de seguridad y privacidad de la información a todas las partes interesadas.

14.18. Articular los proceso y/o áreas involucradas en las diferentes fases de diagnóstico, planificación, operación, evaluación y mejoramiento continuo del Sistema de seguridad y privacidad de la información por parte del área de Sistemas como líder de dicho sistema.

Revisó y aprobó:

Jefe Oficina de Control Interno

Preparó Auditores: Diana del Pilar Romero Varila. Contratista profesional de la Oficina de Control Interno, Cto. 109 de 2023. DR
Jizeth Hael González Ramírez. Contratista profesional de la Oficina de Control Interno, Cto. 100 de 2023. JG