TIPO DE INFORME:	Preliminar		Final	x

Tabla de contenido

Índice de tablas

Índice de ilustraciones

1. TÍTULO DE LA AUDITORÍA

Auditoría de acompañamiento al área de Sistemas – ISO 27001

2. FECHA DE LA AUDITORÍA

Del 1 de abril al 31 de mayo de 2022.

3. PERIODO EVALUADO

Del 1 de enero de 2021 al 30 de marzo de 2022.

4. PROCESO AUDITADO

Gestión de Recursos y Administración de la Información – Sistemas.

5. LÍDER DEL PROCESO / JEFE DE DEPENDENCIA / COORDINADOR

Andrea Paola Sánchez García – Subdirectora Administrativa / Mauris Antonio Ávila Velásquez – Profesional Universitario de Sistemas.

6. AUDITORES

Jizeth Hael González Ramírez / Diana del Pilar Romero Varila.

7. OBJETIVO DE LA AUDITORÍA

Verificar el avance y cumplimiento de los requerimientos de la norma NTC ISO 27001:2013 y demás normatividad asociada como proceso de acompañamiento al área de Sistemas para certificación del proceso de copias de seguridad.

8. ALCANCE

La presente auditoría abarca las actividades y procesos encaminadas a la implementación de Sistemas de Gestión de la Seguridad (SGSI) de conformidad con la Norma Técnica en Capital, en el periodo comprendido entre el 1 de mayo de 2021 y 30 de marzo de 2022. No se realizó evaluación al numeral 6 de la Norma Técnica ISO 27001:2013 relacionado con las actividades de auditoría interna, la formulación y ejecución de acciones que permitan eliminar las causas de las observaciones que se presenten como resultado del presente proceso.

9. CRITERIOS

- Constitución política de Colombia.
- NTC ISO 27001:2013
- NTC ISO 19011:2018
- Modelo de Seguridad y Privacidad de la Información (MSPI) - MINTIC
- Modelo Integrado de Planeación y Gestión - MIPG, Departamento Administrativo de la Función Pública
- Guía para la administración del riesgo y el diseño de controles en entidades públicas
- Manual metodológico para la Administración del riesgo - Canal Capital.
- Política de administración de riesgos - Canal Capital.
- Manual de contratación, supervisión e interventoría – Canal Capital, código: AGJC-CN-MN-001, aprobado mediante Resolución 018 de 2021.
- Caracterización, procedimientos, formatos, manuales y políticas del proceso de emisión de contenidos y demás normatividad vigente aplicable.

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, 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.
- Definición del objetivo, alcance y cronograma de ejecución.
- Preparación de papeles de trabajo de la revisión documental y procedimental sobre la unidad auditada, así como las actividades con procesos adyacentes.
- Preparación de solicitudes de información al área de Planeación y Sistemas.

Ejecución

- Revisión documental de la unidad auditable como la caracterización, formatos, planes, manuales y procedimientos asociados al proceso de copias de información.
- Solicitud de información mediante Memorando inicial, solicitud de soportes sobre los planes de seguridad de la información y riesgos identificados.
- Prueba de recorrido sobre el proceso de copias de información el 11 de mayo de 2022 con el área de Sistemas.

Informe de Auditoría

- Análisis de la información remitida (soportes) por las unidades auditables, en herramienta digital (Drive), información tomada durante la prueba 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 copias de información [Backup].
- Consolidación y entrega del informe preliminar de auditoría a los líderes y/o responsables de la unidad auditable.

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. SITUACIONES GENERALES

11.1. DOCUMENTACIÓN DEL PROCESO

a. AGRI-SI-MN-001, MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI.

Este Manual fue actualizado a su versión 2 en diciembre de 2021, en este documento se establece la metodología que se usará para el diseño del sistema de gestión de seguridad de la información en la entidad conforme a los lineamientos de la NTC ISO 27001:2013.

El documento inicia con la identificación de objetivos, explica qué es y para qué sirve el Sistema de Gestión de Seguridad de la Información, y continúa identificando qué incluye el SSGI, en este capítulo se indica lo siguiente:

- El numeral 5.2 del capítulo 5 se denomina "Procedimientos y Mecanismos que soportan el SGSI", en este se establecen las siguientes 6 etapas de trabajo para elaborar los procedimientos y mecanismos que soportarán el SGSI:

  1. Política de seguridad de la información
  2. Análisis de los requisitos del SGSI

3. Determinar riesgos
4. Analizar los riesgos
5. Valoración de riesgos
6. Declaración de aplicabilidad SOA

Se describe de manera general cada etapa y los requisitos se deben cumplir en cada una de estas, pero no hay información la forma se van a cumplir cada una de estas etapas (responsables, recursos, fechas para el cumplimiento, etc.), es importante adoptar, para cada una de las etapas señaladas en el numeral 5.2, un plan de acción con su respectivo seguimiento, que permita establecer el avance sobre cada una de ellas, en el caso de la política de seguridad de la información podría indicarse por ejemplo que Capital ya cuenta con esta política, que se identifica con el código AGRI-SI-PO-002, que fue aprobada desde 24/09/2022 por el CIGD, que se socializa periódicamente a los funcionarios a través de (…) es necesario ampliar la información y relacionar los documentos que ya se tienen adoptado en el Sistema de Gestión de la Entidad.

De manera adicional se recomienda que el Manual del SGSI sea muy general en su articulación con los demás documentos asociados, ya que cada actualización implicaría su modificación.

5.2.1 Política de Seguridad de la Información

Documento en el cual están establecidos los dominios y controles, que permiten la regulación de la Seguridad de la Información al interior del Canal Capital.

5.2.2 Análisis de los Requisitos del SGSI

De acuerdo con lo establecido en la Norma ISO/IEC 27003:2010 para establecer los requisitos de la seguridad de la información se deben tener en cuenta cinco elementos:[4]

- Identificar los activos de información importantes
- Visión de la Entidad y sus efectos sobre los requisitos futuros.

i este documento se encuentra impreso no se garantiza su vigencia, por lo tanto es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

Página 7 d

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI	CÓDIGO: AGRI-SI-MN-001	ALCALDÍA MAYOR DE BOGOTÁ D.C.
		VERSIÓN: 02	
		FECHA: 13/12/2021	
		RESPONSABLE: SISTEMAS	

- Aplicaciones, Redes, Recursos de TI.
- Requisitos Legales y reglamentarios.
- Conciencia sobre la seguridad de la información.

Fuente: Manual del sistema de gestión de seguridad de la información-SGSI

- El numeral 5.3 denominado "Diseño del SGSI", indica que se deben contemplar 3 componentes para realizar el diseño:

1. Documentación del Sistema
2. Implementación de Controles del Plan de Tratamiento de Riesgos
3. Monitoreo constante de la Seguridad de la Información

Para el componente 1, se muestra una tabla donde se indica la información que debe estar documentada según el requisito técnico de la norma ISO 27000, pero no se evidencian casillas adicionales en las que se registre cómo el área da cumplimiento al requisito normativo relacionado, como se muestra a continuación:

Tabla 1 - Resumen de la Información Documentada para el SGSI

Numeral	ISO-TEC 27001	Documentación
4.3	Determinación del Alcance del SGSI	El alcance debe estar disponible como información documentada.
5.2	Política de Seguridad	La política de seguridad debe estar disponible como información documentada.
6.1.2	Valoración de riesgo de seguridad de la información	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información.
6.1.3	Tratamiento de riesgos de la seguridad de la información	Información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.
6.1.3	Declaración de aplicabilidad	Declaración de aplicabilidad.
6.2	Objetivos de seguridad de la información y planes para lograrlos	Objetivos de la seguridad de la información.

Numeral	ISO-TEC 27001	Documentación
7.2	Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información.
7.5	Información documentada	La que la entidad determine que es necesaria para el SGSI.
7.5.3	Control de la información documentada	La información documentada de origen externo.
8.1	Planificación y control operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo con la planificación.
8.2	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información.
8.3	Tratamiento de riesgos de la seguridad de la información	Resultados de los tratamientos de riesgos de la seguridad de la información.
9.1	Seguimiento, medición, análisis y evaluación.	Evidencia de los resultados del monitoreo y la revisión.
9.2	Auditoria interna	Conservar la información documentada como evidencia de la implementación del programa de auditoria y los resultados de esta.
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por la Dirección.
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada.
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva.

Para los componentes 2 y 3, se recomienda que el área realice la adaptación de la herramienta PDCA (PHVA) identificada con las acciones que deberían implementarse en el marco de la ejecución del SGSI al interior de la organización, con elementos como el plan de tratamiento de riesgos un hito central del modelo MSPI y la NTC ISO 27001:2013, así como de las acciones de monitoreo por parte del proceso.

a. AGRI-SI-PO-002, POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones estableció los lineamientos mínimos y recomendaciones que se sugieren debe tener la política de seguridad y privacidad de la información, con base en esto, se evidenciaron debilidades en la política de Capital, a la cual le falta incluir lo siguiente:

- Describir los pasos y procedimientos para realizar ajustes a la política.
- Explicación de las consecuencias que se pueden tener en caso de que un funcionario, contratista o tercero incumpla la política.

El MinTic también recomienda lo siguiente *"es de gran ayuda* ***incluir la descripción general de otras políticas relevantes para el cumplimiento de los Objetivos planteados dentro del proyecto del SGSI*** *ya que éstas son el apoyo sobre el cual se desarrolla; éstas deben ser descritas de forma sencilla, puntual y muy efectiva"* (Negrilla fuera de texto) dentro de la política seguridad de la información de

Capital no se relacionan las políticas de tratamiento de datos personales y las políticas y controles para la construcción del PETI que forman parte del Sistema de gestión de Calidad y están siendo implementadas.

Adicionalmente, teniendo en cuenta que la entidad se está preparando para certificar el proceso de copias de seguridad, se recomienda incluir dentro de la política de seguridad y privacidad de la información, las responsabilidades que tienen cada uno de los roles identificados: la Gerencia, el Comité Institucional de Gestión y Desempeño de Capital, el Área de Sistemas, los propietarios de la información y los funcionarios, contratistas y terceros usuarios de la información, frente al cumplimiento del procedimiento de copias de seguridad.

b. AGRI-SI-PL-003, PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El plan de seguridad de la información fue aprobado en la sesión 4 del Comité Institucional de Gestión y Desempeño del 16 – 22 de 2020, en el que se indica como instrumento de medición el Modelo de Seguridad y Privacidad de la Información (MSPI) con última fecha de medición 2020, en el cual se evidenciaron debilidades en el levantamiento de información, lo que podría afectar la calificación de la madurez de implementación de las políticas establecidas en materia de seguridad digital. Lo anterior, se presenta en la tabla 1:

Tabla 1. Debilidades MSPI

Criterio	Respuesta	Observación
Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	No se presenta	Se hace necesario que el área adelante la actualización de la actividad, ya que los resultados obtenidos en el documento relacionado como "Autodiagnóstico Gobierno Digital" son la base de construcción de los documentos asociados al proceso de seguridad y privacidad de la información ajustados a la realidad de Capital.
Procedimientos de control documental del MSPI	Se encuentra en el plan del SGSI de la entidad	Verificado el Plan de Seguridad y Privacidad de la información, no se evidencia el procedimiento de control documental.
Riesgos identificados y valorados de acuerdo a la metodología	La entidad cuenta con la matriz de riesgos de seguridad digital	Se viene adelantando el ejercicio de identificación, por lo que se hace necesario verificar las respuestas dadas, concluyendo que Capital no cuenta con identificación de riesgos en materia de seguridad digital
Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	En la política de seguridad y privacidad de la información se encuentra el incumplimiento de la misma	En la política de seguridad y privacidad de la información no se menciona el proceso disciplinario en caso de incumplimiento de las políticas y/o lineamientos establecidos.
Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	El área de sistemas y control interno cuenta con los informes y planes de mejoramiento en el marco de las auditorías realizadas al SGSI.	Si bien desde la Oficina de Control Interno se realizó una evaluación de algunos aspectos relacionados con seguridad de la información durante la vigencia 2020, no se han adelantado auditorías en materia de copias de seguridad [objeto de la presente evaluación], por lo que el presente ejercicio de evaluación se constituye en el primero.
Aceptación de los riesgos residuales por parte de los dueños de los riesgos	En la matriz de riesgos de seguridad digital se realiza la valoración y tratamiento de los riesgos	Se viene adelantando el ejercicio de identificación, por lo que se hace necesario verificar las respuestas dadas, por lo que no es posible establecer el cumplimiento del criterio, cuando el mapa de riesgos definitivo no ha sido adoptado formalmente.

Fuente: Herramienta MSPI, 2020.

Así mismo, se indica en el documento el ciclo de operación y las características del MSPI [requerimiento general], más no se relaciona el nivel en el que se encuentra Capital, como base de identificación del numeral 8. Cronograma de actividades [las cuales tenían fecha de vencimiento el 31 de diciembre de 2021], durante lo corrido de la vigencia 2022, no se cuenta con cronograma de actividades que refuercen las debilidades en la implementación del plan de seguridad en la organización.

Frente al cronograma de actividades, se evidenciaron algunas debilidades respecto a la ejecución de lo programado, lo cual se presenta en la tabla 2:

Tabla 2. Evaluación cronograma de actividades PSI

Fase	Actividad	Se realizó		Observaciones
		Si	No	
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.			Se evidencia la asistencia a la mesa programada para el 26 de mayo de 2021.
	Documentar políticas, procedimientos, lineamientos, instructivos, etc. Asociados al MSPI y Gobierno Digital.	x		Se han venido documentando políticas, procedimientos, instructivos, planes y programas con oportunidad de mejora.
	Desarrollar la matriz de seguridad digital, acorde a la Politice de Gobierno Digital.		x	No se remiten soportes por parte del área, por lo que no es posible determinar el cumplimiento de lo formulado.
	Actualizar Activos de Información.			No es posible determinar dado que el formato fue formalizado en 2020 y la matriz no cuenta con fecha de actualización.
	Elaborar y aplicar la estrategia de comunicación del SGSI.		x	Se evidencian piezas divulgadas a lo largo de la vigencia en materia de seguridad y privacidad de la información; sin embargo, no se evidencia una estrategia de comunicación a implementar del SGSI.
	Implementar controles de seguridad en la plataforma tecnológica de la entidad.		x	Como se menciona en el numeral 11.3 del presente informe el área no cuenta con controles identificados que permitan articularse con los soportes remitidos.
Evaluación y seguimiento	Implementar la herramienta de medición de la política de gobierno digital.			Se evidencia el documento denominado "Autodiagnóstico Gobierno Digital" en el que se realiza la calificación de requisitos en materia de gobierno digital; sin embargo, no se evidencia plan de acción que atienda las debilidades e inexistencias identificadas.

c. AGRI-SI-PL-004, PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El documento fue aprobado en la sesión 4 del Comité Institucional de Gestión y Desempeño del 16 – 22 de diciembre de 2020, en el que determina el plan de tratamiento de riesgos de seguridad y privacidad de la información, así como el cronograma de actividades para la identificación y tratamiento, del cual no se cuenta con evidencias de cumplimiento, [fecha final establecida 2021] dado que al presente ejercicio de evaluación el área no cuenta con riesgos identificados en materia de copias de seguridad [proceso a certificar], por lo que se establece la importancia de realizar el ejercicio a la brevedad posible.

d. AGRI-SI-PD-014, COPIAS DE SEGURIDAD.

Documento actualizado a su versión 10 del 03 de mayo de 2021, en el cual se identifican actividades enmarcadas en el proceso de copias de seguridad; para evaluar el cumplimiento del procedimiento formulado, se adelantó una prueba de recorrido, con la que se obtuvieron los siguientes resultados:

Tabla 3. Resultados prueba de recorrido

CAPITAL - SISTEMA DE COMUNICACIÓN PÚBLICA

OFICINA DE CONTROL INTERNO

PAPEL DE TRABAJO

Auditoría:	Acompañamiento certificación ISO 27001:2013
Periodo evaluado:	2021-2022
IDENTIFICACIÓN DE LA ACTIVIDAD	
Tipo de evaluación:	Revisión
Auditor(es) Responsable(s):	Jizeth González - Diana Romero
Fecha ejecución:	Mayo de 2022
Objetivo:	Verificar el cumplimiento de los procedimientos, planes y manuales formulados en materia de copias de seguridad para Capital.

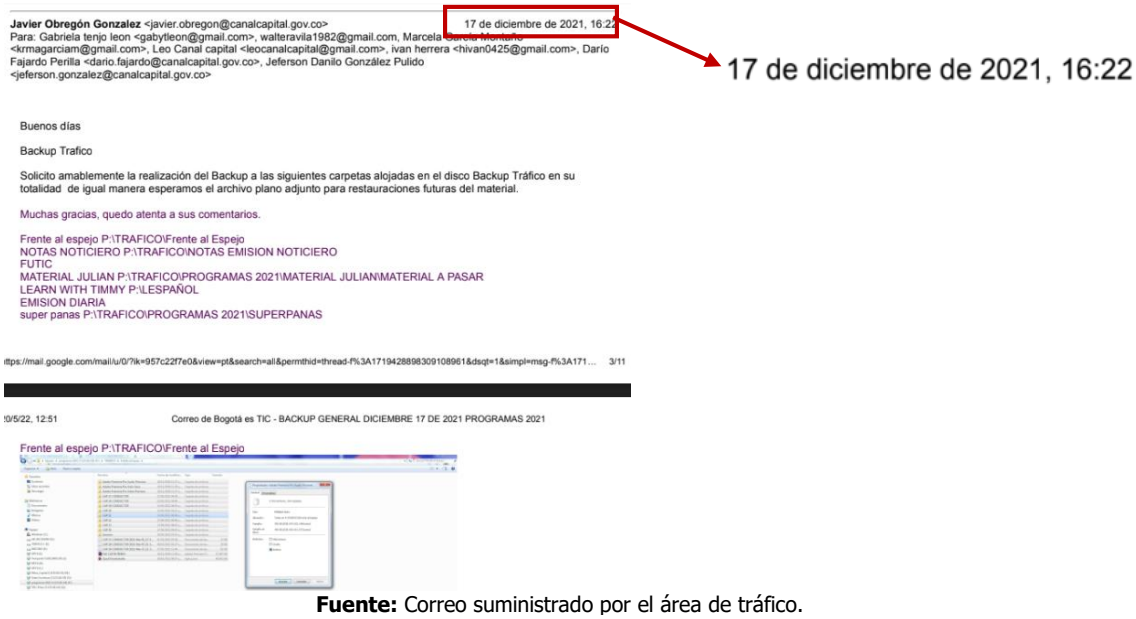
Ítem	Requisito	Cumple		Observaciones
		Si	No	
1	¿Se cuenta con el archivo de solicitud de copias de información del periodo enero 2021 - marzo 2022, de conformidad con el procedimiento de copias de seguridad?	x		Se cuenta con una carpeta dentro del correo sistemas@canalcapital.gov.co dentro de la cual se archivan los correos de solicitud de copias de seguridad.
2	¿Cuál es el método de control para verificar la solicitud de copias de información?			Se cuenta con un formato de google Forms con el que se solicita la información, generando una bitácora de copias de información [39 solicitudes adelantadas]. Como soporte de la actividad se evidencia la tabla de solicitudes [39] indicada durante la evaluación; sin embargo, los correos que soportan la ejecución de las actividades contempladas solo son cinco (5).
3	¿El área cuenta con el archivo de las instrucciones al usuario de conformidad con lo establecido en el procedimiento de copias de seguridad?			No se generan instrucciones al usuario, solo se indica el inicio y la terminación del proceso. Lo cual, una vez verificado en los correos remitidos, solo se adelantó para dos (2) solicitudes.
3	¿Cuáles son los medios disponibles en Capital para realizar la copia de seguridad?			Cintas LTO - Archivadas en el Datacenter - se encuentran contramarcadas y el software indica lo que existe en cada cinta. La herramienta se parametriza.
4	¿El área cuenta con los registros generados sobre la copia de seguridad requerida, teniendo en cuenta lo definido en el procedimiento de copias de seguridad?			Se encuentran en la bitácora.
5	¿El área cuenta con las notificaciones a los interesados sobre la copia solicitada? Remitir soportes.			Correos de respuesta a los solicitantes. De los cuales una vez verificados, solo se evidencia la confirmación en (4) correos y (1) en el que se notifica solo la ejecución de la 1 parte, sobre las adicionales no se registra confirmación.
6	¿Cómo se da la aceptación del usuario sobre el Backup adelantado?			No se remite por parte del usuario una aceptación, solo se indican las fallas evidenciadas. Lo cual no coincide con lo establecido en el procedimiento, actividades 9 y 10.
7	¿Cómo se realiza la gestión documental de los medios disponibles para copias de seguridad de la información?			Informe de copias de seguridad, Inventario de cintas. No se encuentran incluidos en la carpeta digital creada por el área de Gestión Documental. Se realizó la solicitud de los soportes de los informes e inventario de cintas, sobre los cuales solo se recibió el documento denominado "Conjuntos de copias de seguridad por grupo de soportes" en el cual se distingue con dificultad el informe de copias realizado por el programa adquirido para tal fin.

Ítem	Requisito	Cumple		Observaciones
		Si	No	
8	¿Cuál es el protocolo de cierre del caso para copias de seguridad requeridas?			Correo en el que indica que el proceso de copias de seguridad ha finalizado. Lo cual difiere con lo indicado en la actividad 14 del procedimiento establecido.
9	¿Los medios extraíbles indicados en el procedimiento son propiedad del Canal? o del solicitante?, si los medios son del Canal, ¿cómo se lleva el control de la salida de estos elementos?			Los medios extraíbles son del Canal [Solo Cintas LTO], en casos en que el contratista requiera la información se hace el Backup en el medio del contratista.
10	Hacer entrega de la consolidación de los reportes mensuales de las copias de información realizadas.			Correos de respuesta a los solicitantes. Lo cual no se evidencia en los soportes remitidos por el área, incumpliendo lo definido en la actividad 6 del procedimiento de copias de seguridad de servidores.
11	¿Cómo se adelanta el cifrado e integridad de las copias de seguridad realizadas?			El cifrado es opcional y se da por el software - No se encuentran cifrados por ser documentos videográficos, los documentos no se cifran. Por continuidad del negocio no se adelanta el cifrado.
12	¿Con qué frecuencia se adelantan las pruebas de restauración de información?, ¿cuál es el protocolo para realizarlas?			* Como lo indica el ingeniero encargado en el área de Sistemas durante la prueba de recorrido realizada el 11 de mayo *"a diario se adelanta por solicitud vía correo electrónico y se realiza por parte de Digital - Sistemas no adelanta restauraciones de la parte misional"*. * Sistemas restaura documentos y también se adelanta a solicitud. Con lo anterior, se evidencia confusión con el procedimiento de copias de seguridad, ya que lo indicado en el Manual de políticas complementarias, hace referencia a normas de restauración de información, más no de respaldo.
Observaciones del auditor				
* Al verificar que la información se encuentra en la cinta, el programa elimina la copia realizada para dejar espacio libre. * El sistema tiene un sistema de identificación contra sobreescritura. * En el proceso de archivo el robot cuenta con 13 cintas para evitar quedar sin el espacio de almacenamiento.				

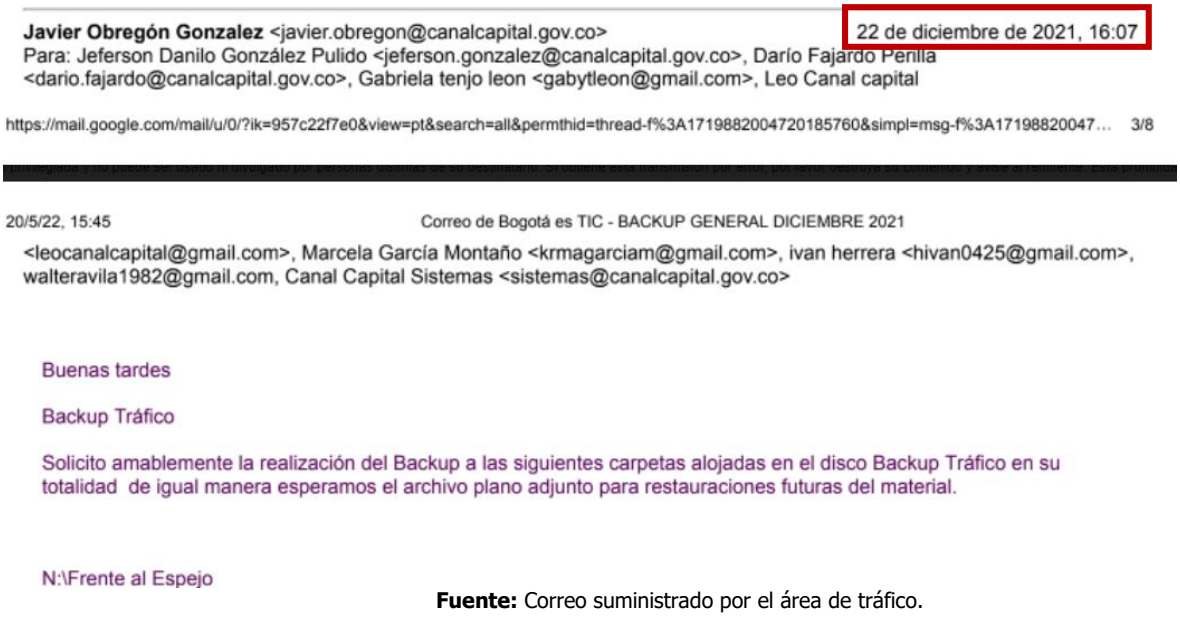
Fuente: Prueba de recorrido 11 de mayo de 2022.

Con los resultados obtenidos, se adelantó la solicitud de soportes frente a las actividades de copias de seguridad, con las que se evidencia el incumplimiento de las actividades 1 – 5 – 7 – 10 y 6 de la copia de seguridad de servidores, ya que lo indicado en el procedimiento no cuenta con evidencia de su ejecución.

Como complemento de lo anterior, se evidenció en el marco de la *auditoría de Diseño y creación de contenidos*, las solicitudes de Backup al área de Sistemas en las fechas del 17 y el 22 de diciembre de 2021, las cuales no se registran en la bitácora mencionada por el área de Sistemas:



Fuente: Correo suministrado por el área de tráfico.



Fuente: Correo suministrado por el área de tráfico.

8/11/2021 11:21:12	ccadmingapps@canalcapital.gov.co	Cindy Ariza - Javier Obregon	T2 El espejo - Backup General	11/08/2021
8/25/2021 10:08:42	ccadmingapps@canalcapital.gov.co	Javier Obregon	ARISE SEAFLOWER - EMISION DIARIA JUNIO 2021 - LEONOR - SOMOS COLOMBIANIDAD	25/08/2021
9/6/2021 16:49:27	ccadmingapps@canalcapital.gov.co	Javier Obregon	BACKUP GENERAL 2 - SEPTIEMBRE 01 de 2021	6/09/2021
9/19/2021 12:37:54	ccadmingapps@canalcapital.gov.co	Javier Obregon	BACKUP GENERAL 3 - SEPTIEMBRE 15 de 2021	19/09/2021
9/23/2021 17:09:52	ccadmingapps@canalcapital.gov.co	Gabriela Tenjo	BACKUP GENERAL 4 - SEPTIEMBRE 21 DE 2021	23/09/2021
10/13/2021 17:08:44	dario.fajardo@canalcapital.gov.co	Javier Obregon	BACKUP GENERAL 6 - 3 OCTUBRE DE 2021	13/10/2021
10/29/2021 11:01:37	dario.fajardo@canalcapital.gov.co	Javier Obregon	BACKUP GENERAL # 7- OCTUBRE 27 2021 FUTIC	29/10/2021
11/25/2021 13:50:30	ccadmingapps@canalcapital.gov.co	Javier obregon	Backup completo 24 de nov	25/11/2021
12/25/2021 14:07:48	dario.fajardo@canalcapital.gov.co	Javier Obregon	Backup Trafico	24/12/2021
12/29/2021 6:40:08	dario.fajardo@canalcapital.gov.co	Javier Obregon	Backup Trafico	29/12/2021
1/18/2022 11:55:42	dario.fajardo@canalcapital.gov.co	Javier Obregon Gonzalez	Contenidos Capital 2022	18/01/2022
1/27/2022 11:17:41	ccadmingapps@canalcapital.gov.co	Javier Obregon	Trafico	27/01/2022

Fuente: Bitácora del área de tráfico.

Lo anterior, podría materializar un riesgo de pérdida de información, teniendo en cuenta que a la fecha la información requerida no ha sido encontrada y restaurada, teniendo en cuenta la cadena de correos

suministrada entre el área de Sistemas y Tráfico, desde el 19 de mayo hasta el 23 de mayo de 2022. Como se observa en la siguiente imagen:

El vie, 20 may 2022 a las 14:01, Javier Obregón Gonzalez (<javier.obregon@canalcapital.gov.co>) escribió:

Cordial saludo, en respuesta a:

"Las razones por las cuales falla un backup derivan de que haga inventario de los archivos a respaldar y al ejecutar la acción de backup los mismos ya no e hasta tanto no sea corregida de manera manual desde tráfico

Dicho esto no se evidencia fallas en los backups realizados en estas fechas por lo cual esta información nunca estuvo disponible para ser respaldada ."

los invito a revisar el siguiente archivo de correo **BACKUP GENERAL DICIEMBRE 17 DE 2021 PROGRAMAS 2021** donde desde mi correo institucional se hizo la sol imagen), del cual no obtuvimos respuesta de parte de los responsables del proceso.

Ahora bien, si dentro del listado requerido por la Oficina de Control Interno existe una fecha de Octubre la cual sí fue encontrada y restaurada y esa carp hicieron parte del mismo Back Up.

Atentamente,

El vie, 20 may 2022 a las 11:45, Germán Darío Fajardo (<dario.fajardo@canalcapital.gov.co>) escribió:

Buen día, de acuerdo con su solicitud iniciamos la búsqueda de los archivos en mención, con el siguiente resultado:

Para describir mejor la imagen se resalta que:

Como se ve en la imagen, no existe información de 30 días comprendidos entre el 30/04/2021 y el 01/06/21; a su vez

La imagen anterior muestra que del 30/06/2021 al 10/10/2021 tampoco hay registro de archivos respaldados en backup .

Es de tener en cuenta que la información referida hace parte de los backups automáticos que realiza el servidor en donde de manera diaria a las 3:00AM selecciona el total de

Fuente: Correo área Tráfico.

De igual manera en el marco de la situación descrita el área no ha identificado en los mapas de riesgo de gestión ni de seguridad digital de la organización este tipo de eventos, ni controles a implementar que permitan mitigar su materialización, así como de planes de acción para tratamiento y su respectivo monitoreo.

Lo que aunado a lo identificado en el numeral 11.3 del presente informe, el proceso de copias de seguridad tiene debilidades que no son monitoreadas, así como tampoco se realizan ejercicios de autoevaluación e implementación de acciones de mejora que permitan mitigar este tipo de eventos que afectan los atributos de disponibilidad e integridad de la información.

e. AGRI-SI-PL-002, PLAN DE CONTINUIDAD DEL NEGOCIO.

El área cuenta con el documento actualizado en su versión 1 del 18 de enero de 2021, en el cual se relacionan criterios sobre los procesos del área; sobre el proceso competente de la presente evaluación en lo que respecta a la actividad de Sistemas de Backup y contingencia de la información, no se evidencia la articulación con el procedimiento ni manual de políticas complementarias, así como tampoco con el manual del SGSI.

Dentro del documento tampoco se evidencian las actividades de contingencia en caso de presentarse incidentes sobre las copias de información, lo cual aunado a que no se cuenta con identificación de riesgos en la materia, se podría materializar la pérdida irrecuperable de información, así como la definición de la ruta a seguir en caso de presentarse.

f. AGRI-SI-GU-007, GUIA DE REPORTE DE INCIDENTES DE SEGURIDAD.

El Ministerio de Tecnologías de la Información y las Comunicaciones emitió la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información, con el propósito de emitir los lineamientos básicos para la puesta en marcha de un sistema de gestión de incidentes en las Entidades Públicas.

Teniendo en cuenta los siguientes incidentes identificados en la guía: *Destrucción no autorizada de información, Robo o pérdida de información o Modificación o eliminación no autorizada de datos*. Estos se pueden mitigar identificando e implementando las actividades del procedimiento Copias de Seguridad.

Se verificó que la guía de reporte de incidentes de Capital, cumpla con los lineamientos básicos y características propuestas por el MinTic. Resultados que se muestran en la tabla No. 4

Ilustración 1. Características de un Modelo de Incidentes de Seguridad de la Información

Fuente: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información MinTic

- **Verificación de los lineamientos básicos de la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del MinTic**

Tabla 4. Lineamientos guía Incidentes de seguridad

Lineamiento de la Guía del Mintic	Guía de Reporte de Incidentes de Capital			
	Cumple			Observaciones
	Si	No	Parcial	
1. Designar un grupo o persona para la gestión de incidentes.		X		No se tiene documentado que personas (cargos o roles) forman parte del grupo de gestión de incidentes, ni sus funciones entre las que se encontrarían las siguientes: • Definir los procedimientos a la atención de incidentes. • Realizar la atención, manejar las relaciones con entes internos y externos. • Definir la clasificación de incidentes.

Lineamiento de la Guía del Mintic	Guía de Reporte de Incidentes de Capital			
	Cumple			Observaciones
	Si	No	Parcial	
2.Procedimientos y programas de capacitación en Gestión de Incidentes			X	Los responsables indican que se encuentra inmerso en el *Plan de sensibilización del sistema de gestión de seguridad y privacidad de la información* Código: AGRI-SI-PL-005, sin embargo, no se evidencian actividades de capacitación explícitamente en gestión de incidentes de copias de seguridad [teniendo en cuenta que el proceso está sujeto a actividades de certificación], por lo que se recomienda adelantar la inclusión de este tipo de capacitaciones. Adicionalmente el plan está formulado con acciones para ser ejecutadas durante la vigencia 2021, no se actualizó el plan para la presente vigencia [2022].
3.Identificación por parte del equipo de TICs de las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones			X	Conforme a lo indicado por los responsables del proceso se aplican buenas prácticas recomendadas desde la Alta Consejería Distrital TIC en temas relacionados con las copias de seguridad, sin embargo, no se tienen documentadas.
4.Información de Contacto: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones		X		La guía de incidentes no tiene esta información, para conocimiento de los colaboradores de la entidad.
5.Política de Comunicación: La entidad debe tener una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.		X		No se observó dentro de los documentos evaluados, una política de comunicación documentada en relación con los incidentes de seguridad.
6.Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque. Tener un diagrama de red para tener la ubicación rápida de los recursos existentes Una Línea – Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente. Se debe tener un análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.		X		Se solicitó al proceso entregar las evidencias, sin embargo, no fueron remitidas a la OCI para su revisión, por lo que no se contó con evidencia que permite concluir de su existencia.
7.listado de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información		X		Se solicitó al proceso entregar las evidencias, sin embargo, no fueron remitidas a la OCI para su revisión, por lo que no se contó con evidencia que permite concluir de su existencia.
8.En capital existe una única fuente de tiempo (Sincronización de Relojes)	X			Se encuentra configurado por el servidor de dominio. NTP
9.Niveles de impacto definidos para catalogar la severidad de los accidentes		X		No se encuentra documentado.

Lineamiento de la Guía del Mintic	Guía de Reporte de Incidentes de Capital			
	Cumple			Observaciones
	Si	No	Parcial	
10. Clasificación de incidentes de Seguridad de la Información	X			
11.Priorización de los Incidentes Y Tiempos de Respuesta en cada caso		X		No se encuentra documentado.
12.Proceso de Notificación de Incidentes			X	Se cuenta con un formato para el reporte de incidentes (AGRI-SI-FT-040), pero en la guía de reporte de incidentes, no se describe el proceso que deben realizar los colaboradores para la notificación de incidentes de copias de seguridad, el formato no se encuentra articulado con la guía.
13.Estrategias para evitar la propagación del incidente y disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.			X	En la guía no están descritas cuáles estrategias implementa el Canal en cada caso (Erradicación, contención y recuperación) para abordar incidentes relacionados con las copias de seguridad.
14. Acciones post Accidente – Repositorio de Lecciones aprendidas.		X		No se encuentran documentado.

De los 14 criterios evaluados la guía de gestión de incidentes de Capital 2 se cumple de manera satisfactoria, tiene implementados parcialmente 4, e incumple con 8. Por lo anterior se hace necesario ajustar el contenido de la guía, incluir la información solicitada y documentar conforme a lo indicado en los diferentes numerales. Adelantando la implementación de las debilidades señaladas se fortalecerá en la guía cada una de las 4 características, que debe tener el *Modelo de Incidentes de Seguridad de la Información* y su proceso de copias de seguridad. De igual manera se recomienda relacionar en la guía los documentos y/o formatos que forman parte del Sistema de Gestión de la entidad y que se articulan con este documento.

g. AGRI-SI-MN-006, MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN.

Canal Capital, cuenta con el documento actualizado con fecha del 10 de diciembre de 2021, en el cual se establece en el numeral 5.17 las políticas de Backup y restauración de información, las cuales, una vez verificadas no permitió evidenciar su articulación con los demás documentos en materia de copias de seguridad, así como tampoco se detallan estrategias o directrices de registro y seguimiento de incidentes de eventos que puedan presentarse sobre las copias de información adelantadas por parte de los responsables del proceso.

De igual manera, en el marco de la implementación de las generalidades identificadas en el documento, el área no adelanta el registro de las pruebas de restauración de información [soportes de ejecución de la actividad] que permita evidenciar la ejecución de las acciones determinadas en caso de presentarse vulneraciones al sistema.

11.2. INDICADORES DEL PROCESO

En el marco de lo evaluado sobre la norma NTC ISO 27001:2013, se adelantó la verificación de los indicadores de eficacia relacionados con la implementación de actividades de seguridad de la información y específicamente en materia de copias de seguridad, sobre lo cual se observa que el registro adelantado de las actividades de ejecución en las hojas de indicadores se mide mediante indicadores de eficiencia más no de eficacia [de conformidad con la norma].

Frente al reporte adelantado que se realiza de las actividades, se observa la falta de mecanismos que permitan soportar la medición fiable y verificable documentalmente de lo indicado por el área de Sistemas trimestralmente durante el monitoreo adelantado por el área de Planeación.

Numerador	Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de seguridad y privacidad de la información	20%	40%	70%	
Denominador	Porcentaje programado de cumplimiento del Plan de seguridad y privacidad de la información para la vigencia	90%	90%	90%	
RESULTADO		22,2%	44,4%	77,8%	

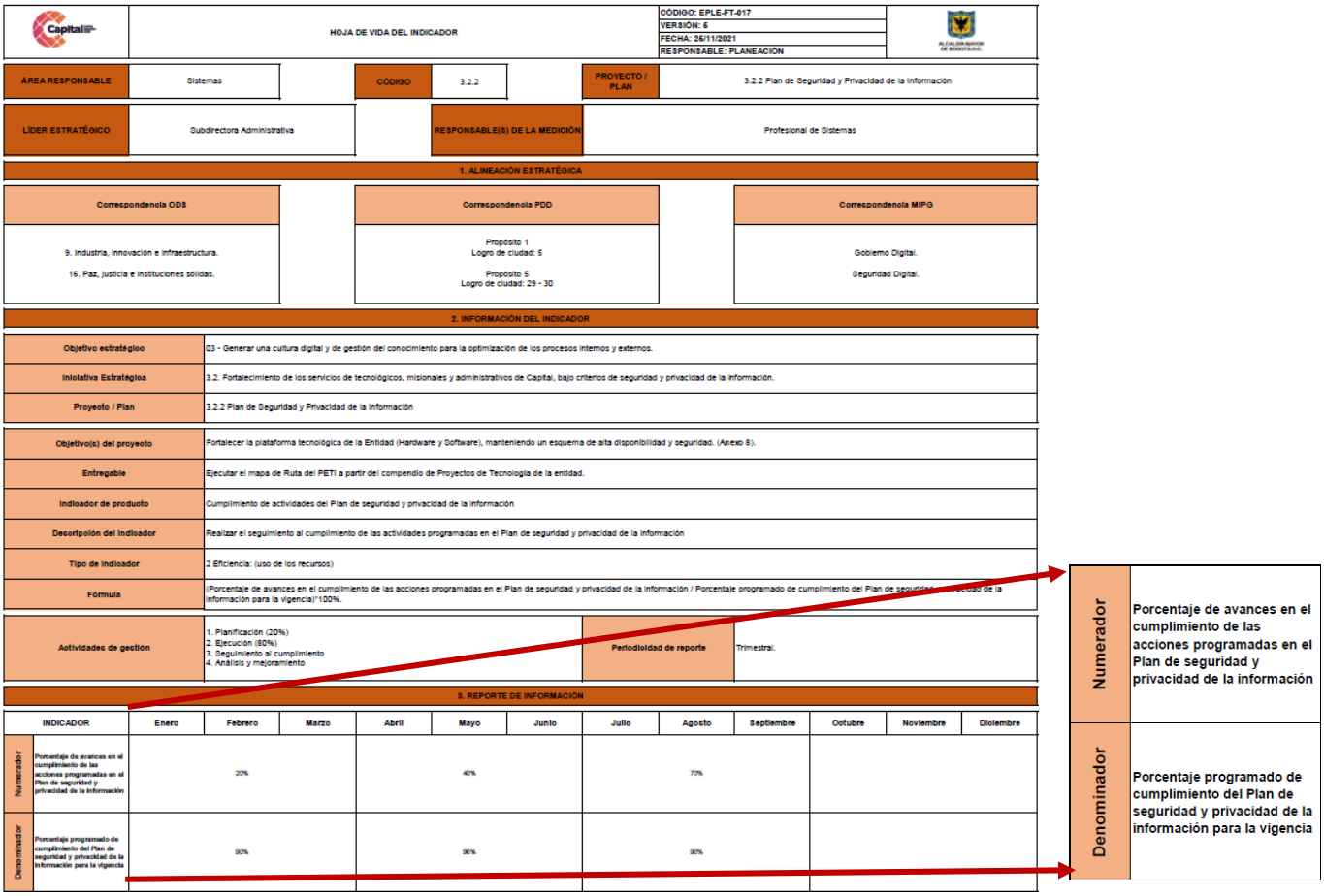
4. ANÁLISIS DE RESULTADOS	
El análisis de resultados en la presente sección debe ser consecuente con los avance obtenidos en el período de seguimiento para el indicador reportado, teniendo en cuenta las actividades de gestión descritas para el mismo.	
SEGUIMIENTO 1	Para el periodo reportado, se realizaron las siguientes actividades acorde al plan de seguridad y privacidad de la información 2021: • Se desarrolló y publicó el plan de seguridad y privacidad de la información AGRI-SI-PL-003 en la intranet de la entidad. • Se actualizaron tres (3) procedimientos (AGRI-SI-PD-014 COPIAS DE SEGURIDAD, AGRI-SI-PD-018 CREACIÓN DE USUARIOS Y EXPEDICIÓN DE CARNÉ INSTITUCIONAL y AGRI-SI-PD-017 SOPORTE TÉCNICO), los cuales se encuentran en proceso de publicación en la intranet de la entidad. • Se elaboró el plan de sensibilización del sistema de gestión de seguridad de la información, este será presentado al comité institucional en el mes de abril, con el propósito de que sea aprobado. • Se han implementado reglas y políticas a nivel de red LAN y WAN en el FIREWALL de la entidad, con el fin de mitigar riesgos de seguridad en los activos de información de la entidad. • Se inició con la revisión de la documentación obligatoria requerida por la NTC/ISO:27001, con el fin de iniciar el proceso de certificación de un proceso de la entidad.
SEGUIMIENTO 2	Para el periodo reportado, se realizaron las siguientes actividades acorde al plan de seguridad y privacidad de la información 2021: • Para el periodo del reporte, se han implementado y documentado reglas y políticas a nivel de LAN y WAN en el FIREWALL de la entidad, lo anterior para salvaguardar la seguridad de la plataforma tecnológica y de la información que es producida y procesada por las áreas de capital en el cumplimiento de las funciones. • Se realizó la actualización AGRI-SI-GU-008 Guía de Acceso y Servicios de Red, debido al cambio de equipos y configuración lógica en la infraestructura tecnológica de la entidad. • Socialización de los procedimientos para el traslado, actualización y seguimiento del inventario de equipos tecnológicos entre las Áreas de sistemas y técnica. • Socialización de la Política de seguridad y privacidad de la información en el marco del plan de capacitación de Talento Humano. • Se elaboró, público y socializó el Plan de Sensibilización del Sistema de Gestión de Seguridad y Privacidad de la Información a través de comunicaciones internas.
SEGUIMIENTO 3	Para el periodo reportado, se realizaron las siguientes actividades acorde al plan de seguridad y privacidad de la información 2021: *Habilitación de política en el equipo de seguridad perimetral (firewall), para la conexión o acceso remoto por medio de la aplicación VPN (forticlient) a la sede 2 chapinero. * Parametrización y configuración de políticas y reglas firewall fortinet 401E: Se configuró política o regla en el equipo de seguridad perimetral (firewall), para publicar la VLAN 1 con el segmento de red 2801:16:6800:100::/64 y VLAN 504 con el segmento de red 2801:16:6800:200::/64. * Se diseñó el documento: CATÁLOGO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN, el catálogo de servicio de TI, es elaborado para que los usuarios de Capital conozcan los servicios de TI que actualmente se encuentran implementados y operativos bajo la administración del área de sistemas, así mismo, en el marco de la implementación de la Política de Gobierno Digital: Catálogo de servicios de TI - LI.ES.11 y a las mejores prácticas de la industria de Tecnología de Información (ITIL®). * Se implementaron medidas preventivas en la infraestructura tecnológica de la entidad, de acuerdo al boletín de seguridad infraestructura critica emitido por el ColCert.

Fuente: Reporte Indicadores Planeación, 2021.

Como se puede observar en las hojas de los indicadores 3.2.2 y 3.2.3, referenciadas previamente, así como en los literales a y b del presente numeral. Teniendo en cuenta lo indicado en la evaluación de los numerales 4-5-7 y 8 de la NTC ISO 27001:2013:

a. Cumplimiento de actividades del Plan de seguridad y privacidad de la información

Ilustración 2. Ficha indicador 3.2.2 - Sistemas



Capital	HOJA DE VIDA DEL INDICADOR		CÓDIGO: EPLE-FT-017 VERSIÓN: 6 FECHA: 26/11/2021 RESPONSABLE: PLANEACIÓN		
ÁREA RESPONSABLE	Sistemas	CÓDIGO	3.2.2	PROYECTO / PLAN	3.2.2 Plan de Seguridad y Privacidad de la Información
LÍDER ESTRATÉGICO	Subdirectora Administrativa	RESPONSABLE(S) DE LA MEDICIÓN	Profesional de Sistemas		

1. ALINEACIÓN ESTRATÉGICA

Correspondencia ODS	Correspondencia PDD	Correspondencia MIPG
9. Industria, innovación e infraestructura. 16. Paz, justicia e instituciones sólidas.	Propósito 1 Logro de ciudad: 5 Propósito 5 Logro de ciudad: 29 - 30	Gobierno Digital. Seguridad Digital.

2. INFORMACIÓN DEL INDICADOR

Objetivo estratégico	03 - Generar una cultura digital y de gestión del conocimiento para la optimización de los procesos internos y externos.
Iniciativa Estratégica	3.2. Fortalecimiento de los servicios de tecnológicos, misionales y administrativos de Capital, bajo criterios de seguridad y privacidad de la información.
Proyecto / Plan	3.2.2 Plan de Seguridad y Privacidad de la información
Objetivo(s) del proyecto	Fortalecer la plataforma tecnológica de la Entidad (Hardware y Software), manteniendo un esquema de alta disponibilidad y seguridad. (Anexo 8).
Entregable	Ejecutar el mapa de Ruta del PETI a partir del compendio de Proyectos de Tecnología de la entidad.
Indicador de producto	Cumplimiento de actividades del Plan de seguridad y privacidad de la información
Descripción del indicador	Realizar el seguimiento al cumplimiento de las actividades programadas en el Plan de seguridad y privacidad de la información
Tipo de indicador	2 Eficiencia: (uso de los recursos)
Fórmula	(Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de seguridad y privacidad de la información / Porcentaje programado de cumplimiento del Plan de seguridad y privacidad de la información para la vigencia)*100%.
Actividades de gestión	1. Planificación (20%) 2. Ejecución (80%) 3. Seguimiento al cumplimiento 4. Análisis y mejoramiento
Periodicidad de reporte	Trimestral.

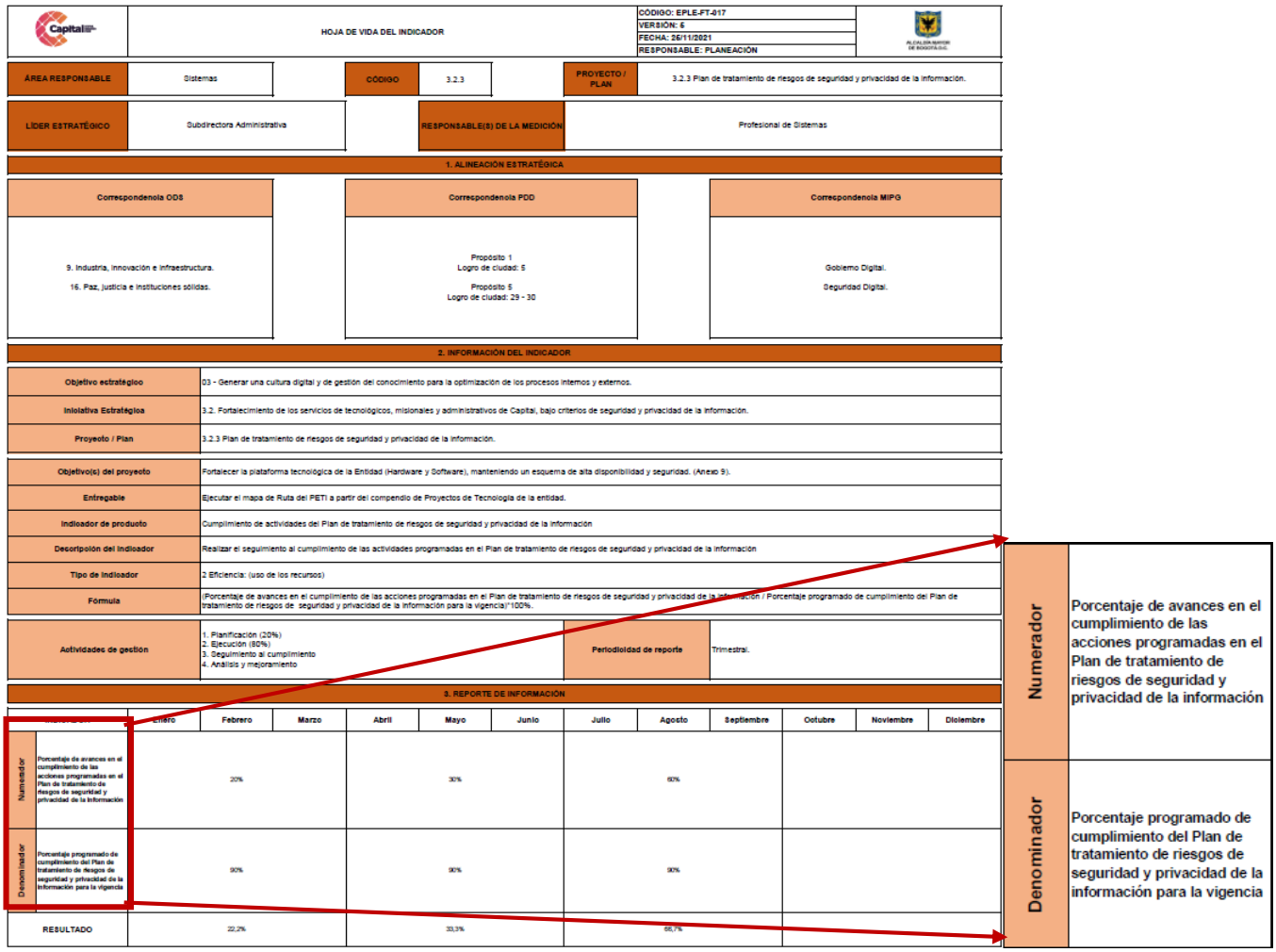
3. REPORTE DE INFORMACIÓN

INDICADOR	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Numerador: Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de seguridad y privacidad de la información		20%			40%			70%				
Denominador: Porcentaje programado de cumplimiento del Plan de seguridad y privacidad de la información para la vigencia		90%			90%			90%				

Numerador	Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de seguridad y privacidad de la información
Denominador	Porcentaje programado de cumplimiento del Plan de seguridad y privacidad de la información para la vigencia

b. Cumplimiento de actividades del Plan de tratamiento de riesgos de seguridad y privacidad de la información.

Ilustración 3. Indicador 3.2.3 - Sistemas



HOJA DE VIDA DEL INDICADOR

CÓDIGO: EPLE-FT-017
VERSIÓN: 6
FECHA: 26/11/2021
RESPONSABLE: PLANEACIÓN

ÁREA RESPONSABLE	Sistemas	CÓDIGO	3.2.3	PROYECTO / PLAN	3.2.3 Plan de tratamiento de riesgos de seguridad y privacidad de la información.
LÍDER ESTRATÉGICO	Subdirectora Administrativa	RESPONSABLE(S) DE LA MEDICIÓN		Profesional de Sistemas	

1. ALINEACIÓN ESTRATÉGICA

Correspondencia ODS	Correspondencia PDD	Correspondencia MIPG
9. Industria, innovación e infraestructura. 16. Paz, justicia e instituciones sólidas.	Propósito 1 Logro de ciudad: 5 Propósito 5 Logro de ciudad: 29 - 30	Gobierno Digital. Seguridad Digital.

2. INFORMACIÓN DEL INDICADOR

Objetivo estratégico	03 - Generar una cultura digital y de gestión del conocimiento para la optimización de los procesos internos y externos.
Iniciativa Estratégica	3.2. Fortalecimiento de los servicios de tecnológicos, misionales y administrativos de Capital, bajo criterios de seguridad y privacidad de la información.
Proyecto / Plan	3.2.3 Plan de tratamiento de riesgos de seguridad y privacidad de la información.
Objetivo(s) del proyecto	Fortalecer la plataforma tecnológica de la Entidad (Hardware y Software), manteniendo un esquema de alta disponibilidad y seguridad. (Anexo 9).
Entregable	Ejecutar el mapa de Ruta del PETI a partir del compendio de Proyectos de Tecnología de la entidad.
Indicador de producto	Cumplimiento de actividades del Plan de tratamiento de riesgos de seguridad y privacidad de la información
Descripción del indicador	Realizar el seguimiento al cumplimiento de las actividades programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información
Tipo de indicador	2 Eficiencia: (uso de los recursos)
Fórmula	(Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información / Porcentaje programado de cumplimiento del Plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia)*100%.
Actividades de gestion	1. Planificación (20%) 2. Ejecución (80%) 3. Seguimiento al cumplimiento 4. Análisis y mejoramiento
Periodicidad de reporte	Trimestral.

3. REPORTE DE INFORMACIÓN

INDICADOR		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Numerador	Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información		20%			30%			60%				
Denominador	Porcentaje programado de cumplimiento del Plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia		90%			90%			90%				
RESULTADO			22,2%			33,3%			66,7%				

Numerador	Porcentaje de avances en el cumplimiento de las acciones programadas en el Plan de tratamiento de riesgos de seguridad y privacidad de la información
Denominador	Porcentaje programado de cumplimiento del Plan de tratamiento de riesgos de seguridad y privacidad de la información para la vigencia

11.3. VERIFICACIÓN ISO 27001:2013

Adelantando la verificación de los lineamientos establecidos en la norma NTC ISO 27001:2013, se realizó la implementación de una lista de chequeo para la evaluación del proceso de copias de seguridad de Capital, con excepción del numeral de auditoría.

Se presenta a continuación en las tablas 5 a 8, el registro de lo observado:

Tabla 5. Requisito 4 de la NTC ISO 27001:2013

CAPITAL - SISTEMA DE COMUNICACIÓN PÚBLICA

OFICINA DE CONTROL INTERNO

PAPEL DE TRABAJO

Auditoría:	Acompañamiento certificación ISO 27001:2013
Periodo evaluado:	2021-2022
IDENTIFICACIÓN DE LA ACTIVIDAD	
Tipo de evaluación:	Revisión
Auditor(es) Responsable(s):	Jizeth González
Fecha ejecución:	Mayo de 2022
Objetivo:	Verificar el grado de cumplimiento de la norma ISO 27001 para el proceso de certificación.

Tabla 5. Requisitos del numeral 4, NTC ISO 27001:2013

Numeral	Requisito	Cumple		Observaciones
		Si	No	
4.2.	**Establecimiento y gestión del SGSI**			
4.2.1	**Establecimiento del SGSI**			
La organización debe:				
a.	Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.			En el Manual del Sistema de Gestión de Seguridad de la Información - SGSI no se establecen: las características del negocio, ni la ubicación. En el numeral 5 del mismo documento se establece el alcance y exclusiones. Sin embargo, dentro del documento no se evidencian los activos, aunque se menciona su identificación como requisito.
b.	Definir una política de SGSI que incluya: 1. Marco de referencia para fijar objetivos, sentido general de la organización y principios para la acción con relación a seguridad de la información. 2. Tiene en cuenta requisitos legales y obligaciones de seguridad contractuales. 3. Alineada con el contexto organizacional de gestión del riesgo. 4. Criterios contra los cuales se evaluará el riesgo. 5. Aprobación por la dirección		x	Capital cuenta con una política de SGSI en la que se contemplan los objetivos, requisitos legales y obligaciones, así como la aprobación por la dirección [Comité Institucional de Gestión y Desempeño] el 24 de septiembre de 2020; sin embargo, esta no contiene el contexto organizacional alineado a la gestión del riesgo, así como tampoco los criterios con los cuales se evaluarán los riesgos que se lleguen a identificar.
c.	Define el enfoque organizacional para la valoración del riesgo: 1. Identifica una metodología de valoración del riesgo. 2. Desarrolla criterios de aceptación de riesgos.	x		Capital cuenta con política de administración de riesgos [EPLE-PO-001], así como con el Manual metodológico de administración del riesgo [EPLE-MN-003] en los cuales se define la metodología de identificación de riesgos y sus niveles de aceptación.
d. - e. - f.	Identificación de riesgos, análisis y evaluación de riesgos y opciones de tratamiento de riesgos [de conformidad con los lineamientos de la ISO 27001:2013].		x	El área viene adelantando el ejercicio de identificación de riesgos de seguridad Digital; sin embargo, para el ejercicio de evaluación sobre el proceso de copias de seguridad se indica por parte de Sistemas que no se cuenta con la identificación de riesgos frente a copias de seguridad en el mapa de riesgos correspondiente, por lo tanto, no se ha documentado la identificación de amenazas, vulnerabilidades, impactos, niveles, aceptación e implementación de controles, en la herramienta correspondiente.

Numeral	Requisito	Cumple		Observaciones
		Si	No	
				Los riesgos que se encuentran en proceso de identificación por parte del área, no se encuentran redactados conforme a lo determinado en los documentos de administración de riesgos de Capital, así como tampoco atienden a lo indicado en la guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020.
g.	Selecciona los objetivos de control y controles para tratamiento de riesgos		x	Teniendo en cuenta que no se ha adelantado un adecuado ejercicio de identificación de riesgos por parte del proceso, no se evidencia la relación de controles.
h.	Aprobación de la dirección sobre los riesgos residuales propuestos.		x	No se ha adelantado el ejercicio de identificación de riesgos.
i.	Autorización de la alta dirección para implementar y operar el SGSI.	x		Los documentos asociados al SGSI como la Política de SGSI fue aprobada por el Comité Institucional de Gestión y Desempeño el 24 de septiembre de 2020.
j.	Cuenta con la elaboración de la declaración de aplicabilidad: a. Objetivos de control y controles, así como las razones para su elección. b. Objetivos de control y controles implementados actualmente. c. Exclusión de cualquier objetivo de control y controles con la debida justificación.			Si bien Capital cuenta con la política de SGSI, así como el manual de SGSI y otros documentos de reporte de incidentes, políticas complementarias y procedimientos de copias de seguridad, no se evidencia la identificación de controles [ni su implementación] ni la exclusión de los que no apliquen, de conformidad con lo requerido en la norma. Es importante, que el área finalice la identificación de los riesgos asociados al proceso evaluado, de manera que se mitigue la materialización de eventos con consecuencias negativas para la organización.
4.2.2	**Implementación y operación del SGSI**			
La organización debe:				
a.	Formular un plan para el tratamiento de riesgos que identifique: a. Acción de gestión apropiada b. Recursos c. Responsabilidades y prioridades de manejo de los riesgos	x		Se cuenta con el Plan de tratamiento de riesgos de seguridad y privacidad de la información aprobado por el Comité Institucional de Gestión y Desempeño realizado el 16 y 22 de diciembre de 2022. Sin embargo, este no contempla los recursos necesarios ni las responsabilidades y prioridades para el manejo de los riesgos. Teniendo en cuenta que este documento debe contemplar las acciones que se definen para reducir o mantener los riesgos en niveles aceptables de conformidad con el contexto organizacional de Capital.
b.	Implementa el plan de tratamiento de riesgos para lograr los objetivos de control, incluyendo: a. Financiación b. Asignación de funciones y responsabilidades		x	Teniendo en cuenta que no se ha adelantado el ejercicio de identificación de riesgos por parte del proceso, no se evidencia la implementación del plan de tratamiento formulado.
c.	Implementa los controles seleccionados para cumplir los objetivos de control		x	Teniendo en cuenta su relación con la respuesta previa, no se evidencia la implementación de controles.
d.	Define cómo medir la eficacia de los controles y cómo se usan para producir resultados.		x	El documento estructurado "Plan de tratamiento de riesgos de seguridad y privacidad de la información" no contempla controles, así como tampoco la eficacia de estos y su uso.
e.	Implementa programas de formación y toma de conciencia.		x	Dentro de las pruebas adelantadas, así como de los soportes remitidos en materia de formación y toma de conciencia, no se evidencian soportes que permitan evidenciar el cumplimiento del requisito para el proceso evaluado.

Numeral	Requisito	Cumple		Observaciones
		Si	No	
f.	Gestiona la operación del SGSI	x		Se cuenta con documentos formulados como el plan de sensibilización del sistema de gestión de seguridad y privacidad de la información, así como del plan de seguridad y privacidad de la información en la que se detallan actividades encaminadas al fortalecimiento del SGSI.
g.	Gestiona los recursos del SGSI	x		Dentro del PETIC se encuentran identificados recursos para el fortalecimiento del SGSI en el capítulo 3. Gestión de seguridad y privacidad de la información, así como en el plan de adquisiciones se registran los recursos requeridos para la contratación del talento humano requerido para implementación del SGSI.
h.	Implementa procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.	[redacted]		El área cuenta con documentos diseñados para el reporte de incidentes como AGRI-SI-GU-007, GUIA DE REPORTE DE INCIDENTES DE SEGURIDAD, AGRI-SI-PD-014, COPIAS DE SEGURIDAD, entre otros. Sobre los cuales se adelantan recomendaciones de revisión y modificación, teniendo en cuenta la operación de la organización.
4.2.3	**Seguimiento y revisión del SGSI**			
La organización debe:				
a.	Ejecuta procedimientos de seguimiento y revisión y otros controles para: a. Detectar errores en los resultados del procesamiento b. Identificar con prontitud los incidentes e intentos de violación, tanto los que tuvieron éxito como los que fracasaron. c. Posibilitar que la dirección determine si las actividades de seguridad delegadas se están ejecutando en la forma esperada. d. Ayudar a detectar eventos de seguridad impidiendo incidentes de seguridad mediante el uso de indicadores. e. Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.	[redacted]		Si bien el equipo del área de sistemas implementa actividades de revisión sobre los resultados de procesamiento de copias de seguridad, incidentes que puedan presentarse, así como de acciones tomadas, sin embargo, no se evidencia la documentación de dichos resultados dentro del Sistema de Gestión de Seguridad de la Información de Capital.
b.	Emprende revisiones regulares de la eficacia del SGSI, teniendo en cuenta resultados de auditorías, incidentes, medición de la eficacia y retroalimentación de las partes interesadas.		x	Teniendo en cuenta que a la fecha no se han adelantado ejercicios previos de auditoría al proceso de copias de seguridad y temas transversales de seguridad de la información, no se evidencian las revisiones regulares de la eficacia del SGSI, así como tampoco se documentan los resultados y retroalimentación de los reportes de incidentes ocurridos.
c.	Mide la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.		x	No se evidencia la identificación de controles, por lo que no se registra la medición de su eficacia durante la vigencia 2021 y lo corrido de 2022 [31 de marzo].
d.	Revisar valoraciones de los riesgos en intervalos planificados, revisar el nivel de riesgo residual y riesgo aceptable, teniendo en cuenta: a. La organización b. La tecnología c. Objetivos y procesos del negocio (amenazas identificadas, eficacia de los controles identificados, eventos externos como cambios en el entorno, obligaciones contractuales y clima social).		x	De conformidad con lo indicado en los literales d, e y f del presente numeral, el área no ha finalizado el ejercicio de identificación de riesgos asociados al proceso evaluado, por lo que no se adelantan las revisiones en intervalos planificados, de conformidad con lo requerido.

Numeral	Requisito	Cumple		Observaciones
		Si	No	
f.	Emprender una revisión del SGSI por la dirección en forma regular asegurando que el alcance sea suficiente y se identifiquen mejoras en el proceso.		x	Teniendo en cuenta lo consignado en el acta de reunión del Comité Institucional de Gestión y Desempeño del 29 de abril de 2021, el área presentó documentos relacionados al SGSI; sin embargo, no se evidencia la presentación de resultados obtenidos de la ejecución del sistema para identificación de mejoras del proceso.
g.	Actualizar los planes de seguridad teniendo en cuenta las conclusiones de las actividades de seguimiento y revisión.		x	Teniendo en cuenta lo indicado en el literal previo, no se han adelantado actualizaciones como producto de las actividades de seguimiento y revisión.
h.	Se registraron acciones y eventos que podrían tener impacto en la eficacia o desempeño del SGSI.		x	De conformidad con lo mencionado en los literales f y g del presente numeral no se han registrado acciones con impacto sobre la eficacia o desempeño del SGSI.
4.2.4	**Mantenimiento y mejora del SGSI**			
La organización debe, regularmente:				
a.	Implementar mejoras identificadas en el SGSI		x	Teniendo en cuenta que, a la fecha, el área de Sistemas no ha adelantado revisiones periódicas, así como tampoco se han adelantado revisiones por la alta dirección en materia de SGSI no se identifican acciones de mejora sobre las lecciones aprendidas o acciones que impacten la eficacia y desempeño del sistema.
b.	Emprender las acciones correctivas y preventivas adecuadas y aplicar las lecciones aprendidas de las experiencias de seguridad.		x	
c.	Comunicar las acciones y mejoras a las partes interesadas.		x	
d.	Aseguran que las mejoras logran los objetivos previstos.		x	
4.3.	**Requisitos de documentación**			
4.3.1.	**Generalidades**			
La documentación debe incluir				
a.	Declaraciones documentadas de la política y objetivos del SGSI (4.2.1, lit. b)	x		Teniendo en cuenta lo indicado en el numeral 4.2.1, los documentos asociados al proceso evaluado están sujetos a implementación de acciones de mejora.
b.	Alcance del SGSI (4.2.1, lit. a)	x		Sin observaciones
c.	Procedimientos y controles que apoyan el SGSI		x	De conformidad con lo indicado en los numerales previos los procedimientos y controles están sujetos a la implementación de acciones de mejora.
d.	Descripción de la metodología de valoración de riesgos (4.2.1, lit. a-g)	x		Teniendo en cuenta lo indicado en el numeral 4.2.1, los documentos asociados al proceso evaluado están sujetos a implementación de acciones de mejora.
e.	Informe de valoración de riesgos (4.2.1, lit. c-g)		x	No se ha culminado la identificación de riesgos por parte del área frente al proceso de copias de seguridad por lo que no se evidencia el informe de valoración de riesgos requerido.
f.	Plan de tratamiento de riesgos (4.2.1, lit. b)	x		Como se indica en el numeral 4.2.1 se cuenta con el plan de tratamiento de riesgos; sin embargo, no se implementa.
g.	Procedimientos para asegurar la eficacia de la planificación, operación y control de los procesos de seguridad de la información y descripción de la medición de los controles (4.2.3)	[redacted]		El área cuenta con documentos diseñados como: • AGRI-SI-MN-001, MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI, AGRI-SI-PO-002, • POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, AGRI-SI-PL-003, • PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, AGRI-SI-PL-004, • PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, AGRI-SI-PD-014, • COPIAS DE SEGURIDAD, AGRI-SI-PL-002, • PLAN DE CONTINUIDAD DEL NEGOCIO, AGRI-SI-GU-007, • GUIA DE REPORTE DE INCIDENTES DE SEGURIDAD, AGRI-SI-MN-006,

Numeral	Requisito	Cumple		Observaciones
		Si	No	
				• MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN En los cuales se establecen procesos de planificación, operación y control de actividades de copias de seguridad de la información de manera transversal. Sin embargo, como se indicó en los numerales previos, los documentos se encuentran sujetos a implementación de acciones de mejora.
h.	Registros exigidos (desempeño del proceso e incidentes de seguridad ocurridos)		x	Si bien a la fecha no se han presentado incidentes de seguridad respecto al proceso de copias de seguridad, el área cuenta con un formato de registro de incidentes, así como una guía de reporte. De igual manera, es importante que dichos documentos se articulen con el fin de que el proceso de reporte quede completo y en armonía con la normatividad aplicable vigente.
i.	Declaración de la aplicabilidad.			La declaración de aplicabilidad del SGSI, se adelanta por parte de Capital mediante la política de SGSI, así como el manual de SGSI y otros documentos de reporte de incidentes, políticas complementarias y procedimientos de copias de seguridad relacionados en dicho documento; sin embargo, no se evidencia la identificación de controles [ni su implementación] ni la exclusión de los que no apliquen dentro de la política, de conformidad con lo requerido en la norma. Es importante, que el área finalice la identificación de los riesgos asociados al proceso evaluado, de manera que se mitigue la materialización de eventos con consecuencias negativas para la organización.
4.3.2.	**Control de documentos**			
Se debe establecer un procedimiento documentado para definir acciones de gestión necesarias para:				
a.	Aprobar los documentos en cuanto a la suficiencia antes de la publicación	x		Capital cuenta con el Manual para el control de documentos institucionales [EPLE-MN-002] aprobado el 15 de diciembre de 2021 en el que se establecen los criterios de publicación, actualización, disponibilidad, clasificación, contenido e identificación; de igual manera, el control se ejecuta mediante el listado maestro de documentos [EPLE-FT-019]. Respecto a la documentación externa se identifica la herramienta de Normograma Institucional en la que se recopilan las diversas normas vigentes aplicables al proceso, el cual se mantiene publicado en la intranet de Capital. Se recomienda al área efectuar la actualización de este incluyendo las guías de implementación del SGSI del MinTic.
b.	Revisar y actualizar los documentos según sea necesario y reaprobarlos	x		
c.	Asegurar que los cambios y el estado de la actualización de los documentos estén identificados	x		
d.	Asegurar que las versiones más recientes de los documentos estén disponibles	x		
e.	Asegurar que los documentos permanezcan legibles e identificables	x		
f.	Asegurar la disponibilidad de los documentos, que se apliquen los procedimientos pertinentes de conformidad con su clasificación.	x		
g.	Asegurar que los documentos de origen externo estén identificados.	x		
h.	Asegurar que la distribución de los documentos esté controlada	x		
i.	Impedir el uso no previsto de los documentos obsoletos	x		
j.	Aplicar la identificación adecuada a los documentos obsoletos, retenidos para cualquier propósito	x		
4.3.3.	**Control de registros**			
Los registros deben				
a.	Estar protegidos y controlados			

Numeral	Requisito	Cumple		Observaciones
		Si	No	
b.	Permanecer legibles, identificables y recuperables			Los registros generados de la implementación del SGSI se encuentran controlados mediante la herramienta de Listado Maestro de Documentos, así como se pueden encontrar publicados e identificables en la intranet de Capital. Respecto a los aspectos de identificación, almacenamiento, recuperación y disposición se evidencia que se viene actualizando la Tabla de Retención Documental (TRD) del proceso, dentro de la cual se recomienda la inclusión de los registros en cada serie documental [según aplique]. Así mismo, respecto al literal d., teniendo en cuenta la prueba de recorrido adelantada el 11 de mayo de 2022, a la fecha no se han reportado incidentes de seguridad sobre el proceso evaluado [copias de seguridad] por lo que no es posible verificar el uso del formato existente para registro de incidentes de seguridad adoptado por Capital.
c.	Estar documentados e implementados los controles para la identificación, almacenamiento, protección, recuperación, tiempo de retención y disposición.			
d.	Llevarse registros del desempeño y casos de incidentes de seguridad.			

Tabla 6. Requisitos del numeral 5, NTC ISO 27001:2013

Numeral	Requisito	Cumple		Observaciones
		Si	No	
5.	**Responsabilidad de la Dirección**			
5.1	**Compromiso de la dirección**			
La dirección debe brindar evidencia de su compromiso, mediante:				
a.	Establecimiento de una política del SGSI	x		Teniendo en cuenta lo indicado en el numeral 4 de la evaluación de la norma ISO 27001:2013, se cuenta con una política definida y adoptada por el Comité Institucional de Gestión y Desempeño mediante sesión del 16-22 de diciembre de 2021, la cual está sujeta a la implementación de acciones de mejora. Así mismo, se menciona la identificación de recursos para el fortalecimiento del SGSI en el PETI y plan anual de adquisiciones de la organización.
b.	Asegurando que se establezcan los objetivos y planes del SGSI	x		
c.	Estableciendo funciones y responsabilidades de seguridad de la información	x		
d.	Comunicando la importancia de cumplir los objetivos de seguridad de la información, conformidad de la política, responsabilidades y necesidades de mejora continua.	x		
e.	Brindando los recursos suficientes para implementar, operar, hacer seguimiento, revisar, mantener y mejorar el SGSI.	x		
f.	Decidiendo los criterios para aceptación de riesgos, niveles de riesgo aceptables.	x		
h.	Efectuando revisiones por la dirección del SGSI.			De conformidad con la evaluación adelantada, desde la vigencia 2021 hasta lo corrido de la vigencia 2022 [31 de marzo] no se evidenciaron revisiones del SGSI por parte de la alta dirección, a excepción de la presentación de documentos para aprobación [Acta comité del 29 de abril de 2021].
5.2.	**Gestión de recursos**			
5.2.1	**Provisión de recursos**			
La organización debe determinar y suministrar los recursos necesarios para:				
a.	Establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI	x		Se definen las actividades de fortalecimiento del SGSI en el Plan de Acción Institucional, sobre el cual se adelanta seguimiento trimestral y dichos reportes consolidados por el área de Planeación se publican en el botón de transparencia de Capital.

Numeral	Requisito	Cumple		Observaciones
		Si	No	
b.	Asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio			Teniendo en cuenta lo indicado en el numeral 4 de la evaluación de la norma ISO 27001:2013, los procedimientos y demás documentos asociados al proceso están sujetos a la implementación de acciones de mejora.
c.	Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.	x		Se cuenta con el Manual de Contratación en su versión 10 del 03 de marzo de 2021, el cual es implementado con apoyo de la Coordinación Jurídica.
d.	Mantener la seguridad suficiente mediante la aplicación correcta de los controles implementados		x	Teniendo en cuenta lo mencionado en el numeral 4, no se evidencia la documentación de controles sobre el proceso evaluado de copias de seguridad.
e.	Llevar a cabo revisiones cuando sea necesario y reaccionar apropiadamente a los resultados		x	No se evidencia la realización de revisiones periódicas del SGSI, de conformidad con lo indicado en el numeral 4 de la norma ISO 27001:2013.
f.	En donde se requiera, mejorar la eficacia del SGSI.		x	No se evidencian revisiones periódicas del SGSI, de conformidad con lo indicado en el numeral 4 de la norma ISO 27001:2013, por lo que no se identifican acciones de mejora que afecten la eficacia del SGSI. De igual manera, se hace necesaria la revisión de los indicadores establecidos para fortalecimiento del sistema, teniendo en cuenta que los formulados no permiten establecer de manera clara los avances y mejoras en materia de seguridad de la información.
5.2.2	**Formación, toma de conciencia y competencia**			
La organización debe asegurar que el personal al que se le asigne responsabilidades del SGSI sea competente, mediante:				
a.	Determinación de las competencias necesarias para el personal que ejecute el trabajo del SGSI	x		Se establece la necesidad de conocimiento en materia de seguridad de la información en los estudios previos de la profesional contratada para tal fin, mediante contrato de prestación de servicios No. 104-2021.
b.	Suministro de formación o realización de otras acciones para satisfacer necesidades	x		Profesional Ingeniero de Sistemas con Especialización en Seguridad de la Información.
c.	Evaluación de la eficacia de las acciones emprendidas.			Se presenta el informe de las obligaciones relacionadas de manera mensual, el cual es aprobado por el supervisor inmediato [Profesional Universitario de Sistemas].
d.	Mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones	x		Se mantiene en el archivo de gestión de la Coordinación jurídica el expediente 104-2021 en el que se archivan los certificados de formación académica en modalidad de pregrado y posgrado.
e.	Asegurar que el personal tiene conciencia de la pertinencia e importancia de las actividades de seguridad de la información y de su contribución al logro de los objetivos del SGSI.			Se enmarca dentro de las obligaciones del contratista la generación de estrategias para implementación de los requisitos en materia de SGSI, así como la medición del nivel de madurez de lo aplicado mediante herramientas como el MSPI e indicadores de cumplimiento de lo formulado en el PETI a cargo de la profesional contratada para tal fin. De igual manera, como se menciona en el literal f del numeral 11.1. del presente informe se hace necesario fortalecer el plan de capacitación del área con el fin de asegurar la interiorización y apropiación del modelo al interior de la organización.

Tabla 7. Requisitos del numeral 7, NTC ISO 27001:2013

Numeral	Requisito	Cumple		Observaciones
		Si	No	
7.	**Revisión del SGSI por la dirección**			
7.1	**Generalidades**			
a.	La dirección debe revisar el SGSI (por lo menos 1 vez al año) para asegurar su conveniencia, suficiencia y eficacia.		x	Dentro de los soportes remitidos, así como de la verificación de las actas entregadas del Comité Institucional de Gestión y Desempeño no se adelantan revisiones por la alta dirección, así como tampoco se identifican oportunidades de mejora o cambios que afecten la eficacia e implementación del SGSI.
b.	Incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos en la política y objetivos de seguridad.		x	
7.2.	**Información para la revisión**			
Las entradas para la revisión deben incluir:				
a.	Resultados de las auditorías y revisiones del SGSI		x	De conformidad con lo indicado en los numerales previos, no se han adelantado acciones de revisión por la dirección, debido a que a la fecha no se cuenta con todas las entradas indicadas en el presente numeral de la norma evaluada [ISO 27001:2013].
b.	Retroalimentación de las partes interesadas		x	
c.	Técnicas, productos o procedimientos que se pueden usar en la organización para mejorar el desempeño y eficacia del SGSI.		x	
d.	Estado de las acciones preventivas y correctivas		x	
e.	Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de los riesgos		x	
f.	Resultados de las mediciones de eficacia		x	
g.	Acciones de seguimiento resultantes de revisiones anteriores por la dirección.		x	
h.	Cualquier cambio que pueda afectar el SGSI		x	
i.	Recomendaciones para mejora		x	
7.3.	**Resultados de la revisión**			
Los resultados de la revisión deben incluir:				
a.	La mejora de la eficacia del SGSI		x	De conformidad con lo indicado en los numerales previos, no se han presentado la revisión de la dirección por lo que a la fecha no se cuenta con el establecimiento de las salidas o resultados de revisión indicadas en el presente numeral de la norma evaluada [ISO 27001:2013].
b.	Actualización de la evaluación de riesgos y del plan de tratamiento		x	
c.	Modificación de los procedimientos y controles que afectan la seguridad de la información, incluyendo cambios: a. Requisitos del negocio b. Requisitos de seguridad c. Procesos del negocio que afectan los requisitos d. Requisitos reglamentarios e. Obligaciones contractuales f. Niveles de riesgo y niveles de aceptación		x	
d.	Recursos necesarios		x	
e.	Mejora a la manera en que se mide la eficacia de los controles.		x	

Tabla 8. Requisitos del numeral 8, NTC ISO 27001:2013

Numeral	Requisito	Cumple		Observaciones
		Si	No	
8.	**Mejora del SGSI**			
8.1.	**Mejora continua**			

Numeral	Requisito	Cumple		Observaciones
		Si	No	
La organización debe mejorar mediante:				
a.	Uso de la política de seguridad de la información	x		Teniendo en cuenta lo determinado por la norma para el presente numeral, se identificó que Capital cuenta con una política de seguridad de la información, así como de unos objetivos [los cuales se encuentran sujetos a implementación de acciones de mejora]. Así como con el informe de auditoría adelantada durante la vigencia 2020 por la Oficina de Control Interno con algunos aspectos en el marco de la política de seguridad digital. Sin embargo, el área no cuenta con la documentación del análisis de los eventos presentados en materia de seguridad de la información, así como tampoco del seguimiento adelantado. De igual manera, no se han identificado y documentado las acciones correctivas y preventivas respecto al SGSI, derivado de su monitoreo y revisión por la Alta Dirección.
b.	Los objetivos de seguridad de la información	x		
c.	Resultados de la auditoría			
d.	Análisis de los eventos a los que se les ha hecho seguimiento		x	
e.	Acciones correctivas y preventivas			
f.	Revisión por la dirección		x	
8.2.	**Acción correctiva**			
El procedimiento documentado debe definir:				
a.	Identificación de las no conformidades	x		Se cuenta con el procedimiento CCSE-PD-001 Plan de Mejoramiento por Procesos en la versión 10 del 06 de mayo de 2021, en el que se identifican las actividades que dan cumplimiento al numeral 8.2. de la NTC ISO 27001:2013.
b.	Determinar las causas de las no conformidades	x		
c.	Evaluar la necesidad de acciones que aseguren que las no conformidades vuelvan a ocurrir	x		
d.	Determinar e implementar la acción correctiva necesarias	x		
e.	Registrar los resultados de la acción tomada	x		
f.	Revisar la acción correctiva tomada.	x		
8.3.	**Acción preventiva**			
El procedimiento documentado debe definir requisitos para:				
a.	Identificar no conformidades potenciales y sus causas		x	Teniendo en cuenta que las acciones preventivas se enmarcan en la gestión del riesgo, tal y como se indica en el presente informe, el área no ha realizado un adecuado ejercicio de identificación, evaluación y seguimiento de riesgos sobre el SGSI, por lo que se estaría incumpliendo el numeral 8.3. de la NTC ISO 27001:2013.
b.	Evaluar la necesidad de acciones que aseguren que las no conformidades ocurran		x	
c.	Determinar e implementar la acción preventiva necesaria		x	
d.	Registrar los resultados de la acción tomada		x	
e.	Revisar la acción preventiva tomada.		X	

12.OBSERVACIONES

N°	OBSERVACIONES
11.1	**DESCRIPCIÓN:** Se presentan debilidades en los documentos establecidos en el marco del proceso de copias de seguridad, respecto a: a. Falta de articulación entre los documentos construidos en el marco de la actividad de copias de seguridad. b. Falta de descripción de actividades, fases o etapas requeridas para la implementación de los lineamientos del Sistema de Gestión de Seguridad de la Información. c. Desactualización de los cronogramas de actividades de los planes de seguridad de la información, políticas complementarias, plan de tratamiento de riesgos y plan de sensibilización. d. Incumplimiento de las actividades identificadas en materia de copias de seguridad [1-5-7 y 8 de copias de seguridad, así como de la actividad 6 del procedimiento de seguridad de servidores]. e. Falta de documentación respecto a las actividades y pruebas definidas en los documentos del área. **CRITERIO DE AUDITORÍA:** • AGRI-SI-PD-014 Copias de Seguridad • AGRI-SI-PL-004, PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. • AGRI-SI-MN-001, MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI. • AGRI-SI-PO-002, POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. • AGRI-SI-PL-002, PLAN DE CONTINUIDAD DEL NEGOCIO. • AGRI-SI-GU-007, GUIA DE REPORTE DE INCIDENTES DE SEGURIDAD. • AGRI-SI-MN-006, MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN. • Norma NTC ISO 27001:2013.
11.2.	**DESCRIPCIÓN:** Debilidades en la identificación de los indicadores [de conformidad con la norma], así como del seguimiento de los indicadores de eficiencia relacionados en el marco de la Seguridad y Privacidad de la Información, teniendo en cuenta que no se cuenta con mecanismos que permitan soportar la medición fiable y verificable documentalmente. **CRITERIO DE AUDITORÍA:** • Fichas de indicadores 3.2.2 – 3.2.3 • Norma NTC ISO 27001:2013
11.3.	**DESCRIPCIÓN:** Debilidades respecto a la implementación de los requerimientos normativos de la norma NTC ISO 27001:2013, numerales 4-5-7 y 8. **CRITERIO DE AUDITORÍA:** • AGRI-SI-PD-014 Copias de Seguridad • AGRI-SI-PL-004, PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. • AGRI-SI-MN-001, MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI. • AGRI-SI-PO-002, POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. • AGRI-SI-PL-002, PLAN DE CONTINUIDAD DEL NEGOCIO. • AGRI-SI-GU-007, GUIA DE REPORTE DE INCIDENTES DE SEGURIDAD. • AGRI-SI-MN-006, MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN.

N°	OBSERVACIONES
	• Norma NTC ISO 27001:2013.
11.1.d.	**DESCRIPCIÓN:** Debilidades sobre la gestión documental de las cintas y demás reportes en materia de copias de seguridad, al no evidenciarse debidamente inventariado y documentado para consulta, lo que conllevó a la materialización del riesgo de pérdida de información [área tráfico]. **CRITERIO DE AUDITORÍA:** • AGRI-SI-PD-014 COPIAS DE SEGURIDAD • Norma NTC ISO 27001:2013.
11.1.b. 11.3.	**DESCRIPCIÓN:** Incumplimiento de los requerimientos normativos en materia de identificación, valoración, evaluación y seguimiento de riesgos en materia de seguridad digital [copias de seguridad] al no evidenciarse la ejecución de las etapas de gestión de riesgos. **CRITERIO DE AUDITORÍA:** • AGRI-SI-PL-004, PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. • AGRI-SI-MN-006, MANUAL DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN. • EPLE-PO-001 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS. • EPLE-MN-003 MANUAL METODOLÓGICO PARA LA ADMINISTRACIÓN DEL RIESGO. • Norma NTC ISO 27001:2013.
5	**TOTAL**

13.CONCLUSIONES

13.1. El área de Sistemas ha venido documentando actividades, planes, procesos y otros aplicables en materia de seguridad y privacidad de la información, de manera transversal al proceso de copias de seguridad.

13.2. El área tiene identificados dos (2) indicadores que apuntan a la gestión de seguridad y privacidad de la información, sobre los cuales se adelantan reportes trimestrales.

13.3. El área cuenta con inversión en tecnología frente al respaldo de información como las cintas LTO, robot y programas de ejecución Backup para la información generada al interior de la organización.

13.4. El área cuenta con la destinación de los recursos y el personal capacitado para la implementación de las directrices en materia de gobierno digital, componente de seguridad y privacidad de la información.

Así mismo, se identificaron acciones con oportunidad de mejora frente al proceso evaluado como:

13.5. Revisar y complementar los requerimientos normativos de los documentos construidos por el área en el marco del proceso de copias de información, así como las mejoras frente a la identificación de los puntos de control de los procedimientos articulados en materia de seguridad y privacidad de la información.

13.6. No se cuenta con la identificación de riesgos de seguridad digital que contemplen el proceso de copias de información que establezcan controles y planes de acción frente a la materialización de estos que puedan afectar de manera negativa la organización.

13.7. Se hace necesaria la revisión de los indicadores formulados de manera que estos atiendan el requerimiento normativo de la ISO 27001:2013, así como el reporte de la información que se adelanta por parte del área frente al cumplimiento de lo formulado.

13.8. Se evidencia la falta de articulación entre los documentos existentes de manera que se evidencie el ciclo que lleva la implementación de los requisitos en materia de seguridad y privacidad de la información.

13.9. El área debe reforzar su plan de capacitaciones con la inclusión de temas clave frente a seguridad y privacidad de la información [copias de seguridad] de manera que se interioricen los conceptos relevantes al interior de la organización, mitigando la ocurrencia de eventos adversos que afecten la operación de Capital.

13.10. Se hace necesario que se adelanten revisiones por parte de la alta dirección sobre las actividades que se vienen implementando frente al SGSI, con el fin de identificar mejoras y ejecutar planes de acción que propendan a incrementar el nivel de madurez de la implementación de los requisitos normativos en materia de seguridad y privacidad de la información.

13.11. Se recomienda adelantar ejercicios de autoevaluación sobre los requisitos normativos de la norma NTC ISO 27001:2013 con el fin de identificar lo faltante, así como las debilidades y tomar las decisiones pertinentes, de manera que, una vez madurado el proceso, se pueda proceder a la certificación proyectada.

14. RECOMENDACIONES

14.1. Realizar la identificación, evaluación y monitoreo [periódico] de riesgos referentes a copias de seguridad de la información como proceso transversal del Sistema de Gestión de la Seguridad de la Información de Capital, articulando los controles requeridos y actividades de control, de conformidad con las herramientas establecidas por Capital en materia de Gestión del Riesgo y la Guía para la administración del riesgo del DAFP, versión 5 [2020]. Así mismo dar un alcance mayor a la gestión de los riesgos de Seguridad de la Información en todas las instancias de Capital atendiendo los lineamientos institucionales.

14.2. Adelantar el ejercicio de revisión, ajuste y formulación de los indicadores de eficacia del Sistema de Gestión de Seguridad de la Información de conformidad con lo requerido con la NTC ISO 27001:2013.

14.3. Revisar y articular los diferentes documentos emitidos en materia de SGSI, así como complementar su contenido de conformidad con lo requerido en la normatividad vigente aplicable.

14.4. Adelantar las revisiones por parte de la alta dirección con el fin de que se identifiquen las acciones de mejora preventivas y correctivas del SGSI y con base en ello asegurar la conveniencia, suficiencia y eficacia del sistema.

14.5. Incluir en el plan de capacitación (articulado con el *Plan de Sensibilización del Sistema de Gestión de Seguridad de la Información*) los temas de interés que abarquen los diferentes componentes del modelo de seguridad y privacidad de la información con alcance a todos los colaboradores de la organización, teniendo en cuenta lo determinado en la normatividad vigente aplicable.

14.6. Fortalecer las acciones en materia de gestión documental de manera que se asegure la correcta organización, clasificación y disposición de la información respaldada por parte del área de Sistemas. Así como la debida documentación de la ejecución de las actividades establecidas al interior del proceso de copias de seguridad con el fin de mitigar riesgos.

14.7. Adelantar revisiones periódicas a las herramientas de medición de madurez del SGSI con el fin de identificar las actividades pendientes de ejecución y de mejora e implementar los planes de acción correspondientes que conlleven a la disminución de las brechas existentes en materia de seguridad y privacidad de la información.

Revisó y aprobó:

Jefe Oficina de Control Interno

Preparó
Auditores: Diana del Pilar Romero Varila – Profesional Oficina de Control Interno. DR
Jizeth Hael González Ramírez – Profesional Oficina de Control Interno. JG

Nota:
Usted cuenta con diez (10) días hábiles contados a partir del recibo del presente informe para formular el Plan de Mejoramiento resultado de las cinco (5) observaciones encontradas en la auditoría, empleando para ello el formato CCSE-FT-001 Formulación Plan de Mejoramiento, remitirlo a Control Interno para su validación, aprobación e incorporación de las acciones en la Matriz de Seguimiento del Plan de Mejoramiento [CCSE-FT-019].