



COMUNICACIÓN INTERNA

Bogotá D.C., miércoles 01 de noviembre de 2023

PARA: Luis Felipe Calero González
Secretario de Cultura, Recreación y Deporte (E)

Viviana Margarita Bayuelo Serrano
Jefe Oficina de Tecnologías de la Información

Carlos Alfonso Gaitán Sánchez
Jefe Oficina Asesora de Planeación

Jaime Andrés Tenorio
Tascón Subsecretario de Gobernanza

Leonardo Garzón Ortiz
Director de Arte, Cultura y Patrimonio

Rafael Eduardo Tamayo Franco
Director de Lectura y Bibliotecas

Adriana María Cruz Rivera
Directora de Gestión Corporativa y Relación con el Ciudadano

Margarita María Rúa Atehortúa
Jefe Oficina Jurídica

Ángela María Canizalez Herrera
Jefe Oficina Asesora de Comunicaciones

DE: Omar Urrea Romero
Jefe Oficina de Control Interno

ASUNTO: Informe Final de Auditoría al Sistema de Gestión de Seguridad de la Información y Seguridad Digital en la SCRD.

Estimados Integrantes del Comité de Coordinación de Control Interno,

Para su lectura e información, remito el informe final de auditoría de la referencia.





Como resultado del trabajo realizado se presentan los siguientes:

TIPO DE RESULTADO	CANTIDAD	REFERENCIACIÓN
Cumplimientos	0	N/A
Incumplimientos	1	I01 - Pág. 16
Oportunidades de Mejora	13	OP1, OP2, OP3, OP4, OP5, OP6, OP7, OP8, OP9, OP10, OP11, OP12, OP13 - Páginas 23 a 27
TOTAL:	14	

Tabla N°1 Elaboración propia. Resultados generales del seguimiento.

Es muy importante reconocer las estrategias y actividades desarrolladas por la Secretaría en cabeza, principalmente, de la Oficina de Tecnologías de la Información, demostrando un sólido compromiso que apunta al aumento del nivel de madurez y el cumplimiento de los lineamientos establecidos por el MINTIC para el sistema de seguridad de la información en las entidades públicas. Se evidencia igualmente un avance significativo en los temas evaluados en comparación con los resultados de la vigencia anterior.

Cabe resaltar que existen algunos aspectos que requieren intervención y que son susceptibles de mejora, los cuales se encuentran descritos en las Oportunidades que se identifican en el informe. Al respecto, se destacan los siguientes aspectos:

1. Establecer un proceso de revisión y monitoreo para asegurar el cumplimiento de los lineamientos nacionales en materia de seguridad y privacidad de la información.
2. Fortalecer la información explicativa y la evidencia documental que se presenta por parte de la entidad en referencia a cada requisito descrito en el instrumento de identificación de línea base compartido por el MINTIC, toda vez que se encontraron algunas debilidades o ausencias de soportes que daban cuenta del cumplimiento de los requisitos.
3. Generar los planes de acción necesarios para iniciar la atención de los requisitos con calificación baja, principalmente los relacionados con ciberseguridad.
4. Continuar e intensificar, a nivel institucional, la cultura, conciencia y apropiación en materia de seguridad de la información, por medio de estrategias y campañas donde a todo el personal se refuercen los conceptos y la aplicación de los controles, para así evitar la materialización de riesgos y la explotación de las vulnerabilidades, por parte de externos, que pretendan afectar la ejecución de la misionalidad.
5. Optimizar los procesos y adicionar nuevos ítems derivados de la evaluación de riesgos que continuamente se realiza, incluyendo una revisión más frecuente y detallada de las





amenazas potenciales, alineadas con la realidad operativa de la Secretaría.

6. Crear nuevos controles encaminados a la protección de datos sensibles o tipificados como críticos en la entidad, tales como datos personales de ciudadanos, empleados y contratistas.

Finalmente, se recomienda a la Oficina de Tecnologías de la Información y demás áreas que apoyan este sistema, avanzar en la formulación y ejecución de las acciones que resultan pertinentes para atender las oportunidades de mejora identificadas.

Atentamente,

Omar Urrea Romero
Jefe Oficina de Control Interno.

Adjunto: Informe Final Detallado de Auditoría

Documento 20231400466243 firmado electrónicamente por:	
Omar Urrea Romero	Jefe Oficina de Control Interno Oficina de Control Interno Fecha firma: 01-11-2023 14:38:56
 fd730170ea08b00028c9fefc295e10d6f50f9789299a60eb210a4b6b86871558 Codigo de Verificación CV: d3911	



	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

TABLA DE CONTENIDO

1. DESCRIPCIÓN GENERAL	3
2. CRITERIOS DE AUDITORÍA	3
3. METODOLOGÍA	4
4. LIMITACIONES	4
5. RESULTADOS DEL TRABAJO DE AUDITORÍA	5
5.1. <i>Seguimiento al informe de emitido por la Oficina de Control Interno en la vigencia 2022:</i>	5
Incumplimiento N°1: Falta del ítem informe de solicitudes de acceso a la información, contemplado en el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 que reglamenta la ley 1712 de 2014, dentro de la página web en la sección de transparencia.	16
5.2. <i>Estado de implementación del modelo de privacidad y seguridad de la información en la SCRD:</i>	16
5.3. <i>Evaluación de efectividad de controles - ISO 27001:2013 anexo a:</i>	17
5.4. <i>Instrumento de identificación de la línea base de seguridad:</i>	20
Oportunidad de mejora N°1: Falta de aprobación de documento de autoevaluación por parte de la Alta Dirección.	23
Oportunidad de mejora N°2: Falta de aprobación con el resultado de la herramienta de encuesta de diagnóstico de seguridad y privacidad de la información, por parte de la Alta Dirección.	23
Oportunidad de mejora N°3: Falta de aprobación de documento con la estratificación de la Entidad, por parte de la Alta Dirección.	23
Oportunidad de mejora N°4: Inexistencia de procedimiento oficial para control documental del MSPI en la entidad.	23
Oportunidad de mejora N°5: Debilidades respecto a los acuerdos contractuales (con contratistas) donde se establecen responsabilidades de las partes en referencia a seguridad de la información.	23
Oportunidad de mejora N°6: Inexistencia de plan de capacitación y sensibilización de seguridad de la información para la vigencia 2023, aprobado por la Alta Dirección.	23
Oportunidad de mejora N°7: Falta de soporte con el Inventario de áreas de procesamiento de información y telecomunicaciones.....	24
Oportunidad de mejora N°8: Falta de soporte con el diagrama de red de alto nivel o arquitectura de TI.....	24
Oportunidad de mejora N°9: Falta de Inventario de partes externas o terceros a los que se transfiere información de la entidad.	24
Oportunidad de mejora N°10: Falta de Formato de acuerdo de transferencia de información.	24
Oportunidad de mejora N°11: Inexistencia de Indicadores oficiales de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	24
Oportunidad de mejora N°12: Falta de Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	24
5.5. <i>Ciberseguridad:</i>	24
Oportunidad de mejora N°13: Aspectos relacionados con ciberseguridad con calificación 0 dentro de la entidad.	25

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

6.	CONCLUSIONES	25
7.	RECOMENDACIONES	26
8.	PLAN DE MEJORAMIENTO	27
9.	FIRMAS	27

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

1. DESCRIPCIÓN GENERAL

NOMBRE DE LA AUDITORÍA	Seguimiento al estado del Sistema de Gestión de Seguridad de la Información y Seguridad Digital en la SCRD.
TIPO DE AUDITORÍA	Auditoría de Seguimiento
UNIDAD (ES) AUDITABLES	Oficina de Tecnologías de la Información
RESPONSABLE (S)	Viviana Margarita Bayuelo Serrano
OBJETIVO	Realizar seguimiento al estado del sistema de gestión de seguridad de la información y seguridad digital de la Entidad.
ALCANCE	El proceso de evaluación se enmarcó en la información oficial publicada en la página web de la entidad, así como lo contenido dentro de los procedimientos y la documentación en el sistema integrado de gestión
PERIODO DE EJECUCIÓN	Julio a Septiembre de 2023
EQUIPO AUDITOR¹	Diego Alexander Urazán Franco

2. CRITERIOS DE AUDITORÍA

- Resolución No 596 de 2017, estatuto de auditoría interna y el código de ética de la auditoría Interna de la Secretaría de Cultura, Recreación y Deporte.
- Decreto Único Reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones -MinTic.
- Decreto 767 del 2022 Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución MinTic 500 de 2021, en la que se establecen los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, entre otros.

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

- Documento Maestro del Modelo de Seguridad y Privacidad de la Información MinTic.
- Norma técnica colombiana NTC ISO/IEC 27001.
- Manual de políticas de seguridad y Privacidad de la información de la Secretaría de Cultura, Recreación y Deporte.
- GOT-MN-02 Manual para la identificación y clasificación de activos de información.
- DES-MN-04 V1 Manual de Gestión de Riesgos de Seguridad de la Información

3. METODOLOGÍA

Para el desarrollo del presente seguimiento, se ejecutaron las siguientes técnicas de auditoría:

- Validación de página web y documentación publicada en el sistema integrado de gestión.
- Entrevista.
- Requerimientos de información.
- Análisis, revisión, verificación, validación, contraste y cotejo de información.
- Consolidación y construcción de informe de seguimiento.

4. LIMITACIONES

Durante el proceso de seguimiento ejecutado por el equipo auditor, se informa que no se presentaron limitaciones que hayan afectado la capacidad para obtener evidencia de auditoría adecuada, suficiente y clara.

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

5. RESULTADOS DEL TRABAJO DE AUDITORÍA

En la actualidad, la seguridad y privacidad de la información son preocupaciones cruciales para cualquier entidad pública. La creciente amenaza de ciberataques y la necesidad de cumplir con regulaciones cada vez más estrictas hacen que la protección de los datos y en sí la seguridad sea una prioridad. Bajo este contexto, este informe de auditoría de seguimiento presenta los resultados de la evaluación realizada desde la Oficina de Control Interno a la implementación del Modelo de Seguridad y Privacidad de la información en la Secretaría de Cultura, Recreación y Deporte, identificando y exponiendo las medidas existentes, las situaciones, puntos de mejora y las recomendaciones, determinadas por el equipo auditor.

Como primera medida, se enfatiza que la auditoría se basa en muestreo aleatorio y procedimientos selectivos, lo que implica que existe un margen de riesgo inherente, por ende, nuestras pruebas y evaluaciones nos permitieron formarnos una opinión razonable respecto al objetivo planteado.

Una vez culminado el trabajo de campo y bajo el contexto y los criterios normativos, la Oficina de Control Interno, a continuación, se permite presentar los resultados obtenidos, así:

TIPO DE RESULTADO	CANTIDAD	REFERENCIACIÓN
Cumplimientos	0	N/A
Incumplimientos	1	I01 - Pág. 16
Oportunidades de Mejora	13	OP1, OP2, OP3, OP4, OP5, OP6, OP7, OP8, OP9, OP10, OP11, OP12, OP13 - Páginas 23 a 27
TOTAL:	14	

Tabla N°1 Elaboración propia. Resultados generales del seguimiento.

5.1. Seguimiento al informe de emitido por la Oficina de Control Interno en la vigencia 2022:

A continuación, se presentan los resultados derivados del seguimiento realizado e informado por la Oficina de Control Interno a través del informe de auditoría en la vigencia 2022 de la

 ALCALDÍA MAYOR DE BOGOTÁ D.C. <small>SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE</small>	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

siguiente manera:

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

Resultado informe 2022 emitido por la OCI	Seguimiento 2023 realizado por la OCI
<p>OPORTUNIDAD DE MEJORA: Actualizar el contexto:</p> <p>Se sugiere actualizar el documento denominado “Análisis de Contexto Sector Cultura, Recreación y Deporte 2021”, con el objetivo de incluir en el análisis del contexto de la Secretaría la variable relacionada con la Seguridad y Privacidad de la Información, de tal manera que tengan en cuenta los objetivos propuestos en el SGSI, la madurez de los procesos, los potenciales riesgos que se evidencien, los controles propuestos a los activos de información identificados y se aborden las necesidades de todas las partes interesadas en la Secretaría.</p>	<p>Como respuesta a esta oportunidad de mejora, la OTI a través de memorando de Orfeo número 20231600214903 respondió lo siguiente: Se realizará solicitud a la Oficina de Planeación la inclusión en el documento “Análisis de Contexto Sector Cultura, Recreación y Deporte 2021” la variable relacionada con la Seguridad y Privacidad de la Información, de tal manera que tengan en cuenta los objetivos propuestos en el SGSI, la madurez de los procesos, los potenciales riesgos que se evidencien, los controles propuestos a los activos de información identificados y se aborden las necesidades de todas las partes interesadas en la Secretaría.</p> <p>Para este aspecto, la OTI informa en sesión de validación que dicho tema quedará cubierto en la presente vigencia, es decir, que el tema se está trabajado y se ha acogido lo recomendado por la OCI. Actualmente se está realizando un ejercicio de actualización a la documentación, por lo tanto, este punto queda sujeto a validación y verificación antes de finalizar la presente vigencia.</p>
<p>OPORTUNIDAD DE MEJORA: Objetivos del SGSI:</p> <p>Se sugiere desarrollar, en la fase de “Planificación”, los objetivos, alcance y límites del Sistema de Gestión de Seguridad de la Información (SGSI) alineados con los objetivos del MSPI, que se pretenden implementar en la Secretaría, de tal manera que se integren los procesos misionales, ubicaciones físicas, terceros (operadores), infraestructura tecnológica propia y la administrada por terceros, de acuerdo con lo propuesto en el numeral “8.2 Fase de planificación” del documento denominado “Modelo de seguridad y Privacidad de la Información ” propuesto por el MINTIC y lo</p>	<p>De acuerdo a validación realizada al plan de seguridad y privacidad de la información publicada en la página web de la entidad, fue incluido por parte de la OTI el ítem Construcción de documento de objetivos del SGSI. Adicional y basado en la información suministrada en sesión de trabajo por los responsables de seguridad de la información en la entidad, este documento fue construido, por tanto la oportunidad de mejora fue acogida y atendida por la entidad.</p>

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		INFORME DE AUDITORIA INTERNA	
		FECHA: 18/05/2022	

<p>descrito en la cláusula 1.0 del estándar ISO 27001:2013.</p>	
<p>OPORTUNIDAD DE MEJORA: Formalizar el rol del responsable de la seguridad de la información:</p> <p>Se sugiere formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en la SCRD, transversal a la entidad y cercano a la dirección, de acuerdo con lo propuesto en los numerales “3.2.1.4. Política de seguridad digital” del manual operativo de MIPG y “7.2.3 Roles y responsabilidades” del documento Maestro del Modelo de Seguridad y Privacidad de la Información, que establecen que “se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección”</p>	<p>Para tal fin y a través de la Oficina de Tecnologías de Información para la vigencia 2023, dentro del Plan Anual de Adquisiciones, se incluyó un proceso de contratación para un profesional adscrito a esta Oficina y quien se encargará de la gestión respecto al tema de seguridad la información, contratista que actualmente se desempeña como Oficial de Seguridad de la Información en la entidad; como información adicional, se informa que el contrato culmina en el mes de diciembre de esta vigencia. De acuerdo con lo anterior, el tema fue atendido por la entidad.</p>
<p>OPORTUNIDAD DE MEJORA: Formalizar la asignación de recursos para el desarrollo del MSPI:</p> <p>Se sugiere la asignación de recursos propios para el desarrollo e implementación del Modelo de Seguridad de la Información en la Secretaría, esto, con el propósito de lograr el cumplimiento de los objetivos propuestos a mediano y largo plazo, como lo indica el numeral “5.1 Compromiso de la dirección” del documento denominado “Manual de Políticas de Seguridad y Privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte (GOT-MN-01)”</p>	<p>En la vigencia 2023 la entidad, a través de la Oficina de Tecnologías de la Información, asignó recursos para incluir dentro del plan anual de adquisiciones 2 contratos; el primero hace referencia al oficial de seguridad de la información perteneciente a la mencionada oficina y el segundo corresponde a un profesional asignado a la Oficina de Control Interno, el cual se encargará de realizar evaluaciones a la implementación del modelo de privacidad y seguridad la información en la SCRD. De acuerdo con lo anterior, la entidad atendió la oportunidad de mejora acogiendo la recomendación sugerida.</p>
<p>OPORTUNIDAD DE MEJORA: Activos de información</p> <p>Se sugiere finalizar con el levantamiento de activos de información para concluir con la evaluación y valoración de los riesgos de Seguridad y Privacidad de la Información en la Secretaría. Se encontró que esta actividad</p>	<p>Dentro del plan de seguridad y privacidad de la información fue contemplado la actualización de los activos de información para la vigencia 2023 en la entidad, adicionalmente el equipo de la OTI informa que todas las actividades y sesiones con las dependencias estimadas en dicho plan fueron realizadas, para el momento del seguimiento</p>

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

<p>no se ha desarrollado en la dirección de “Lectura y Bibliotecas” y los plazos propuestos en el “Plan de Seguridad de la Información” de la SCRD finalizaron el 30 de noviembre de 2022.</p>	<p>y de acuerdo con la información suministrada en sesión de trabajo, el tema se encuentra en consolidación de la información recopilada en dichas sesiones. Por lo anterior, nos permitimos informar que la oportunidad de mejora está siendo atendida. No obstante, y de acuerdo a la fecha en la que se realiza el proceso de seguimiento, se sugiere culminar el proceso de actualización de activos de información y publicarlos oficialmente en la página web de la entidad.</p>
<p>OPORTUNIDAD DE MEJORA: Gestión de riesgos:</p> <p>Se sugiere finalizar la evaluación y valoración de los riesgos de Seguridad y Privacidad de la Información a la totalidad de activos de información identificados en la Secretaría. La evaluación se sugiere hacer por cada tipología de riesgo, es decir, por pérdida de integridad, por pérdida de disponibilidad y por pérdida de confidencialidad, así como por cada proceso y por cada activo o grupo de activos (de acuerdo con el tipo) de información, como lo indica la Política de Administración de Riesgos (DES-POL-01), el Proceso (DESPR- 09) y el Manual (DES-MN-04) de “Gestión de Riesgos de Seguridad de la Información” de la Secretaría. En esta valoración se sugiere mantener similitud en los nombres de los campos “tipo de activo” encontrados la lista de activos de información y en las matrices de riesgo de la Secretaría. Se encontró que el tipo de activo denominado “Bases de datos personales” se escribe de manera diferente en el campo “tipo de activos” de las matrices de riesgo (DB Personales), lo que podría confundir al analista de riesgos durante la evaluación de estos activos.</p>	<p>Para el tema de la gestión de riesgos, la entidad ha desarrollado durante la presente vigencia 3 actividades, así:</p> <ul style="list-style-type: none"> * Apoyo e identificación de riesgos de seguridad; este tema se encuentra contemplado e incluido dentro del plan de seguridad y privacidad de la información y se encuentra en proceso. * Elaboración y publicación de la guía para riesgos de seguridad digital. * Finalmente, está en proceso de elaboración de un procedimiento para la gestión de riesgos de seguridad digital. De acuerdo con lo mencionado, el tema para la presente vigencia ha sido atendido, sin embargo, será sujeto de validación posterior por parte de esta oficina.
<p>OPORTUNIDAD DE MEJORA: Tratamiento de los riesgos de seguridad de la información:</p>	<p>La OTI, en la vigencia 2023, respondió lo siguiente: <i>“Esta oportunidad de mejora fue incluida en el actual PLAN DE TRATAMIENTO DE RIESGOS DE</i></p>

	<p>PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN</p>	<p>CÓDIGO: SEG-PR-02- FR-03</p>	<p>*RAD_S* Radicado: RAD_S Fecha: F_RAD_S</p>
	<p>INFORME DE AUDITORIA INTERNA</p>	<p>VERSIÓN: 01</p>	
		<p>FECHA: 18/05/2022</p>	

<p>Se sugiere la elaboración del documento denominado “tratamiento de riesgos” de seguridad de la información, en el cual se deberán listar los riesgos de seguridad asociados a cada proceso y la selección de controles que se utilizarán para mitigarlos. El documento deberá estar aprobado por los líderes de cada proceso, en el entendido que se utilizará como base en la fase de “Operación y/o implementación” del MSPI en la Secretaría.</p>	<p><i>SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023 – en la actividades “Apoyo en la identificación de riesgos de seguridad y privacidad de la información en los activos de información”, “Construcción del procedimiento para identificación, valoración y tratamiento de riesgos de seguridad de la información”, “ Construcción del documento guía para el tratamiento de riesgos de seguridad y privacidad de la información”, que de acuerdo al cronograma establecido y publicado esta para la fecha de 17/11/2023.”</i></p> <p>Una vez expresado lo anterior, se observa que dentro del plan de tratamiento de riesgos de seguridad y privacidad de la información se contempla lo enunciado en la respuesta; no obstante, aun se encuentra en ejecución y desarrollo de actividades, por tal motivo este tema será objeto de seguimiento antes de finalizar la presente vigencia.</p>
<p>OPORTUNIDAD DE MEJORA: Formalizar procesos, guías e instructivos del MSPI:</p> <p>Se sugiere formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI de la Secretaría. Como se evidenció, existe un conjunto de 26 políticas descritas en el documento “Manual de Políticas de Seguridad y Privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte (GOT-MN-01)”, sin embargo, se deberán documentar a través de procedimientos, manuales, guías o instructivos, en las que se describan los lineamientos que se deberán ejecutar para gestionar la Seguridad de la Información en la SCRD.</p>	<p>Según memorando generado por la Oficina de Tecnologías de la Información con número 20231600214903, y específicamente respecto a este aspecto fue contestado que:” <i>Esta oportunidad de mejora fue incluida en el actual PLAN DE SEGURIDAD DE LA INFORMACIÓN 2023 – Actividad “Documentar procedimientos, manuales, guías e instructivos para aplicación de las políticas de seguridad de la información”, que de acuerdo al cronograma establecido y publicado esta para la fecha de 30/11/2023.”</i></p> <p>Según lo expuesto, esta Oficina se permite informar que la entidad continúa en construcción de los documentos complementarios y relacionados que soportan el tema de seguridad y privacidad de la información de la entidad, para tal fin este aspecto será validado posteriormente, de acuerdo con la fecha propuesta en la respuesta por la OTI.</p>
<p>OPORTUNIDAD DE MEJORA: Actualizar</p>	<p>Al validar la declaración de aplicabilidad, la</p>

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

<p>“declaración de aplicabilidad”</p> <p>Se sugiere actualizar y hacer la revisión del documento denominado “Declaración de Aplicabilidad Anexo A ISO 27001:2013”, de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI y los requerimientos actuales de la SCRD.</p>	<p>entidad informa que actualmente se tiene el documento publicado y está pendiente de actualización; adicionalmente, en el mes de mayo fue respondido por la OTI que esta oportunidad de mejora será ejecutada con la actualización de la declaración de aplicabilidad vigente; por lo mencionado el tema será validado por la Oficina de Control Interno antes de finalizar la presente vigencia</p>
<p>OPORTUNIDAD DE MEJORA: Plan de capacitación, sensibilización y comunicación:</p> <p>Se sugiere continuar con el plan de capacitación, sensibilización y comunicación para la vigencia 2023, en el cual se debería involucrar de manera activa al área de Comunicaciones y la de Gestión de Talento Humano, para efectos de evidenciar la participación de la totalidad de empleados / contratistas de la SCRD.</p>	<p>En el plan de seguridad y privacidad de la información publicado en la página de web y en la intranet se tiene contemplado la construcción del plan de capacitación y su correspondiente seguimiento. Adicionalmente y de acuerdo a la respuesta emitida por la OTI en la presente vigencia, la cual describe que: <i>Esta oportunidad de mejora fue incluida en el actual PLAN DE SEGURIDAD DE LA INFORMACIÓN 2023 – en la actividad “Seguimiento del Plan de Capacitación y Sensibilización en Seguridad y Privacidad de la Información I Semestre 2023”, que de acuerdo al cronograma establecido y publicado esta para la fecha de 15/12/2023.</i></p> <p>Basado en lo anterior, este tema queda sujeto a verificación y seguimiento por parte de la Oficina de Control Interno en el mes de diciembre de 2023.</p>
<p>OPORTUNIDAD DE MEJORA: Documentos alojados en dos “menús” de Cultunet:</p> <p>Se sugiere revisar y evaluar la continuidad de dos (2) ubicaciones (menús) en la intranet de la SCRD denominada “Cultunet”, para alojar las políticas, procesos, procedimientos, manuales y formatos, relacionados con el sistema de gestión documental. Resulta confuso encontrar documentos con diferentes versiones que hacen referencia a una misma caracterización o proceso, por ejemplo, se encontró publicado desde el 11 de junio de 2019, en la ruta de “Cultunet”: menú “MIPG”,</p>	<p>Como respuesta dentro del orfeo numero 20231600214903, la OTI informa que <i>“En consideración a la reciente reestructuración de la Secretaría y la actualización de los procesos y procedimientos, la OTI en la actualidad cuenta con un solo proceso denominado “Gestión de Tecnologías de la Información y las comunicaciones” y en la en la ruta de “Cultunet”: menú “MIPG/Documentación del Sistema de Gestión - MIPG/Procesos de apoyo/Gestión de Tecnologías de la Información y las comunicaciones, se encuentra toda la documentación relacionada con el proceso y con Seguridad de la Información”.</i></p>

	<p>PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN</p>	<p>CÓDIGO: SEG-PR-02- FR-03</p>	<p>*RAD_S* Radicado: RAD_S Fecha: F_RAD_S</p>
	<p>INFORME DE AUDITORIA INTERNA</p>	<p>VERSIÓN: 01</p>	
		<p>FECHA: 18/05/2022</p>	

<p>título “Documentación transitoria de los procesos V.8” □ Procesos de apoyo □ Gestión de TIC el documento denominado “Procedimiento de Seguridad Digital (PR-TIC-05), similar a otro encontrado en la ruta: menú “MIPG”, título “Actualización de la documentación de los procesos V.9” □ Procesos de apoyo □ Gestión operativa de TI, denominado manual para la identificación y clasificación de activos de información (GOT-MN-02).</p>	<p>De acuerdo con la revisión realizada dentro de la intranet, se visualiza una única fuente donde se tiene reportado la documentación del proceso gestión de tecnologías de la información y las comunicaciones, por tanto y de acuerdo a lo mencionado, la oportunidad de mejora fue atendida por la entidad.</p>
<p>OPORTUNIDAD DE MEJORA: La OTI y el rol de seguridad de la Información como parte de la segunda línea de defensa de la SCRD:</p> <p>Se sugiere agregar, como parte integral de la segunda línea de defensa, a la Oficina de Tecnología e Información (OTI) y al rol de Seguridad y Privacidad de la Información de la SCRD como áreas de monitoreo y supervisión, como apoyo a la Oficina Asesora de Planeación (OAP). Los controles tecnológicos y de seguridad que ejercerían estas dos áreas serían transversales a la Secretaría y se estaría dando alcance a lo indicado en el título “Segunda línea de defensa” de la 7ª dimensión de Control Interno del Manual Operativo de MIPG.</p>	<p>En referencia a este aspecto, la OTI contestó en radicado N° 20231600214903 que “Se realizará solicitud formal a la Oficina de Planeación integrar en la segunda línea de defensa, a la Oficina de Tecnologías de Información (OTI) y al rol de Seguridad y Privacidad de la Información de la SCRD como áreas de monitoreo y supervisión, como apoyo a la Oficina Asesora de Planeación (OAP).”</p> <p>Para este aspecto, se validó dentro del manual de políticas de seguridad y privacidad de la información de la entidad, en el capítulo 6.1.1. Roles y responsabilidades para la seguridad de la información, las actividades y responsabilidades que debe ejecutar la Oficina de Tecnologías de la Información frente al tema de seguridad de la información, todo esto como parte de la segunda línea de defensa. A manera de ejemplo, se menciona que la definición del rol del oficial de seguridad de la información, el cual se encuentra adscrito a dicha oficina y también se mencionan las siguientes actividades dentro del rol de la OTI:</p> <ul style="list-style-type: none"> ● Coordinar y velar por el cumplimiento de los compromisos establecidos en el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información. ● Gestión para la implementación de políticas, lineamientos, normas, estándares y procedimientos sobre seguridad informática. ●

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

	<p>Gestión para la adquisición y administración de las herramientas de seguridad informática necesarias para el aseguramiento y/o monitoreo de la infraestructura tecnológica de la Entidad. ● Participación en la identificación y mitigación de riesgos y vulnerabilidades de seguridad y privacidad de la Información. ● Gestión de proyectos de seguridad y privacidad de la información. ● Gestión de incidentes en seguridad y privacidad de la Información. ● Realizar revisiones periódicas a los sistemas de información y establecer los controles, medidas técnicas y organizativas al interior de la entidad. ● Informar al Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información acerca del desempeño del SGSPI. ● Elaborar y enviar las actas de reunión y someterlas a aprobación por los miembros que conforman el Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información. ● Convocar las reuniones del Equipo Técnico de Gestión y Desempeño Institucional de Seguridad de la Información, por solicitud del líder del Comité.</p> <p>Expuesto lo anterior, en referencia los roles de la OTI, nos permitimos informar que la oportunidad de mejora ha sido subsanada por parte de la entidad.</p>
<p>OPORTUNIDAD DE MEJORA: Indicadores del MSPI:</p> <p>Se sugiere implementar un procedimiento para gestionar los indicadores y monitorizar las actividades de la implementación de Modelo de Seguridad y Privacidad de la Información en la Secretaría, de acuerdo con lo dispuesto en la fase 4 “Evaluación y desempeño”, con el objetivo de medir el desempeño y eficiencia del sistema.</p>	<p>En el seguimiento realizado por el equipo auditor en la vigencia 2023, se evidencia dentro del documento plan de seguridad y privacidad de la información https://culturarecreacionydeporte.gov.co/sites/default/files/2023-06/tic-pn-02_plan_de_seguridad_y_privacidad_de_la_informacion.pdf 2 procesos de mediciones de indicadores de seguridad de la información para el segundo semestre de 2022 y el I semestre 2023. No obstante, y de acuerdo con lo validado, los indicadores de seguridad y privacidad la información continúan en construcción por parte de la Oficina de Tecnologías de la Información, para lo cual se sugiere culminar las actividades estimadas</p>

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

	frente al proceso de construcción y oficialización de estos indicadores, para así dar inicio con la medición.
OPORTUNIDAD DE MEJORA: Auditorías internas: Se sugiere incluir en el Plan Anual de Auditoría Interna (PAAI) la evaluación periódica del Modelo de Seguridad y Privacidad de la Información – MSPI que se pretende implementar en la SCRD, esto con el objetivo de dar cumplimiento a lo dispuesto en la fase 4 “Evaluación y desempeño” del MSPI.	Dentro del plan anual de auditoría interna de la vigencia 2023, la Oficina de Control Interno incluyó un proceso de evaluación y seguimiento a la implementación del modelo de seguridad y privacidad de la información en la entidad, el cual es verificado reflejado en el presente informe, por lo mencionado, la oportunidad de mejora fue tenida en cuenta y subsanada en el marco de la presente anualidad.
OPORTUNIDAD DE MEJORA: Publicación de documentos de acuerdo con el decreto 612 del 4 de abril de 2018: No se publicó en la página web de la Secretaría de Cultura, Recreación y Deporte – SCRD el “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información” y el “Plan de Seguridad y Privacidad de la Información”, de acuerdo con lo descrito en los numerales 11 y 12 del artículo 2.2.22.3.14 del Decreto 612 del 4 de abril de 2018.	En el vínculo https://culturarecreacionydeporte.gov.co/es/transparencia-acceso-informacion-publica/informacion-entidad/procesos-y-procedimientos/procesos-apoyo/gestion-tecnologias-informacion-comunicaciones la entidad realizó la publicación del plan de tratamiento riesgos de seguridad y privacidad de la información y el plan de seguridad y privacidad de la información de acuerdo con lo validado por el equipo auditor; por lo mencionado, la oportunidad de mejora fue acogida por la entidad.
INCUMPLIMIENTO: Publicación de documentos de acuerdo con el decreto 1081 del 2015: No se evidenció actualizado ni publicado en el sitio web de la Secretaría de Cultura, Recreación y Deporte – SCRD, el “Registro de Activos de Información” y el “Índice de Información Clasificada y Reservada”, durante los años 2020, 2021 y 2022, de acuerdo con lo descrito en el numeral 2.1.1.2.1.4, del Decreto 1081 de 2015 que reglamenta la ley 1712 de 2014. La publicación que se encontró actualmente hacer referencia al registro de activos de información del año 2019.	Se realiza revisión de la página web encontrando que dentro del vínculo https://culturarecreacionydeporte.gov.co/es/transparencia-acceso-informacion-publica/datos-abiertos/registros-de-activos-de-informacion se encuentra publicado el registro de activos de la vigencia 2020, mencionando que para la vigencia 2023 no se ha realizado la publicación del mencionado registro. En segundo lugar, dentro del vínculo https://culturarecreacionydeporte.gov.co/es/transparencia-acceso-informacion-publica/datos-abiertos/indice-de-informacion-clasificada-y-reservada se evidencia publicado el índice correspondiente a la vigencia 2022. Por lo mencionado anteriormente, la entidad

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

	<p>ha subsanado puntualmente el incumplimiento expuesto en el informe de auditoría de la anterior vigencia, no obstante, se sugiere continuar con el monitoreo y validación continua a través de las vigencias para garantizar el cumplimiento de este aspecto normativo.</p> <p>Ahora bien, se declara un nuevo incumplimiento en el sentido que al validar completamente dentro de la página web de la entidad el artículo 2.1.1.2.1.4, del Decreto 1081 de 2015 que reglamenta la ley 1712 de 2014, no se encuentra el correspondiente al numeral 7 titulado informe de solicitudes de acceso a la información.</p> <p>Los siguientes son los ítems que describe el artículo:</p> <ul style="list-style-type: none"> (2) El Registro de Activos de Información. (3) El índice de Información Clasificada y Reservada. (4) El Esquema de Publicación de Información. (5) El Programa de Gestión Documental. (6) Las Tablas de Retención Documental. (7) El informe de solicitudes de acceso a la información.
--	---

Tabla N°2 Elaboración propia. Fuente: Informe de auditoría emitido por la OCI en 2022 Radicado Numero 20221400541903.

Una vez realizado el seguimiento que se describe en la anterior tabla, en resumen, se informa que las oportunidades de mejora se encuentran en trámite o fueron atendidas por la entidad dentro de la presente vigencia, por tanto, es importante continuar con su seguimiento y monitoreo para garantizar su cumplimiento a cabalidad. Después de esto, a continuación, se presenta un nuevo incumplimiento en referencia a la publicación de la información en el botón de transparencia, así:

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

Incumplimiento N°1: Falta del ítem informe de solicitudes de acceso a la información, contemplado en el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 que reglamenta la ley 1712 de 2014, dentro de la página web en la sección de transparencia.

El detalle de este incumplimiento se registra en la última fila de la anterior tabla.

5.2. Estado de implementación del modelo de privacidad y seguridad de la información en la SCRD:

Teóricamente y como se reportó en el informe de la vigencia 2022 por parte de esta Oficina, de manera cíclica el modelo de privacidad y seguridad de la información en las entidades públicas se compone de 5 fases, a mencionar:

-  Diagnóstico
-  Planificación
-  Implementación.
-  Evaluación de desempeño.
-  Mejora continua.

Bajo el contexto anterior y con el fin de realizar un comparativo de avance en la implementación a nivel de la Secretaría, a continuación, se presentan los resultados de la vigencia 2022 seguido del reporte de la vigencia 2023 suministrado por la Oficina de Tecnologías de la Información, así:

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	20%	40%
	Implementación	4%	20%
	Evaluación de desempeño	3%	20%
	Mejora continua	2%	20%
TOTAL		30%	100%

Tabla N°3 Fuente: Informe de auditoría emitido por la OCI en la vigencia 2022 radicado numero 20221400541903

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	27%	40%
Implementación	11%	20%
Evaluación de desempeño	11%	20%
Mejora continua	10%	20%
TOTAL	59%	100%

Tabla N°4 Elaboración propia Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrado por la OTI en agosto de 2023.

Como se contextualizó, al realizar el comparativo entre lo presentado en la vigencia 2022 versus la vigencia 2023 y de acuerdo con la gestión adelantada dentro de la entidad, se incrementó el porcentaje de avance en un **29%**, pasando del **30%** al **59%**. Específicamente para cada componente, en planificación se incrementó 7 puntos, en implementación 7 puntos, en evaluación de desempeño 8 puntos y en mejora continua 8 puntos porcentuales.

Con estos resultados para 2023 se superó la mitad del porcentaje que estipula el ciclo PHVA del Modelo de Seguridad y Privacidad de la Información. También, con los resultados presentados se observa que la entidad avanza transversalmente en todos los componentes, por medio de la ejecución de las actividades y estrategias planteadas de acuerdo con la planeación estimada al inicio de la vigencia. Frente a los porcentajes esperados, principalmente se menciona la brecha existente en el componente de planificación puesto que, por ser la primera fase del modelo, aún presenta una diferencia de 13 puntos porcentuales respecto al total del avance; seguidamente los componentes de implementación y evaluación de desempeño se encuentran a 9 puntos de su cumplimiento y el componente de mejora continua se encuentra en la mitad, es decir a 10 puntos de la meta esperada.

5.3. Evaluación de efectividad de controles - ISO 27001:2013 anexo a:

Durante el ejercicio de seguimiento fue solicitado a la OTI el reporte de los controles estipulados en la norma internacional ISO 27001:2013, específicamente dentro del anexo A, con el fin de validar el estado de implementación a nivel de la entidad y así poder establecer el grado de madurez. A continuación, se presenta el reporte resumido:

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	



Gráfica N°1 Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica actualizado por la OTI en agosto de 2023.

La anterior gráfica muestra el estado actual de cumplimiento y/o adopción de los controles contenidos en la norma ISO 27001 en la Secretaría. Se puede observar que los temas donde se visualiza mayor cumplimiento son políticas de seguridad de la información, organización de la seguridad de la información, seguridad de los recursos humanos, gestión de activos, control de acceso, relación con los proveedores y cumplimiento. Ahora bien, respecto a los aspectos sobre los cuales se requiere enfatizar en la ejecución de las actividades y el enfoque de los esfuerzos por la valoración obtenida, entre otros aspectos se mencionan:

- Criptografía.
- Seguridad física y del entorno.
- Seguridad de las operaciones.
- Seguridad de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información de la gestión de continuidad del servicio.

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

A continuación, se presenta la tabla con la información después de evaluada la efectividad de los controles y el nivel obtenido, dentro de los cuales se mencionan: gestionado, efectivo, repetible y optimizado:

No.	Evaluación de Efectividad de controles	
	DOMINIO	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	GESTIONADO
A.9	CONTROL DE ACCESO	GESTIONADO
A.10	CRIPTOGRAFÍA	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	EFFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	EFFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	EFFECTIVO
A.18	CUMPLIMIENTO	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		GESTIONADO

GESTIONADO	50%
EFFECTIVO	36%
REPETIBLE	7%
OPTIMIZADO	7%

Tablas N°5 y N°6 Elaboración propia Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrado por la OTI en agosto de 2023.

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

5.4. Instrumento de identificación de la línea base de seguridad:

Número	Descripción	Comentario y recomendación OCI
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la Alta Dirección.	El instrumento de evaluación fue actualizado por la OTI en el mes de agosto de 2023 conteniendo la información derivada de la gestión y las actividades adelantadas en la entidad. No obstante, no se evidencia un documento resultado de la autoevaluación realizada propiamente en la entidad que cuente con la aprobación de la alta dirección. Por tanto, se recomienda que dentro de la vigencia 2023, se presente el avance realizado a la alta dirección para que se cuente con su aprobación tal como lo describe el instrumento de línea base.
9	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	Al momento de la evaluación no se cuenta con el documento aprobado y aceptado por la Alta Dirección; por tal motivo, se sugiere ejecutar esta tarea tal como lo describe el instrumento de línea base en su capítulo de levantamiento de información.
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	Al igual que el ítem anterior, no se identifica este documento aceptado y aprobado por la Alta Dirección. Por ende, se recomienda realizar la respectiva generación del documento, presentarlo al Despacho y obtener su aprobación.
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	Como soporte para este aspecto, la entidad cuenta con la política general de seguridad de la información versión uno publicada tanto en la intranet como en la página web. Sin embargo, al validar los tres aspectos que solicita este numeral, los cuales son objetivos, alcance y límites, la política de seguridad de la información de la entidad no describe claramente cuáles son los límites. Por tanto, se recomienda que en la actualización que se realiza a dicha política se tenga en cuenta este aspecto.
12	Procedimientos de control documental del MSPI	Como soporte de este aspecto, la entidad relaciona la caracterización del proceso de gestión estratégica de TI, sin embargo, no se evidencia

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

		puntualmente la existencia de procedimientos en donde se controle los documentos relacionados con el modelo de seguridad y privacidad de la información en la entidad. Por lo mencionado, se recomienda realizar una revisión de este aspecto y generar dentro del sistema integrado de gestión de la entidad el procedimiento relacionado.
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	<p>La Entidad, en el instrumento de identificación, argumenta para este tema que “Actualmente se encuentra vigente en la cláusula nueve de los contratos de los contratistas”. La cláusula 9 dentro del documento condiciones especiales de los contratos describe lo siguiente: “En caso de que exista información sujeta a reserva legal, las partes deben mantener la confidencialidad de esta información. Para ello, el supervisor del contrato debe comunicar al contratista que la información suministrada tiene el carácter confidencial.”</p> <p>Basado en lo anterior, la oportunidad de mejora se presenta debido a que la cláusula 9 hace referencia a información con reserva legal / confidencial, sin contener un lineamiento puntual para todos los tipos de información distinta a esta tipología. Debido a esto, se recomienda reforzar para el tema de seguridad de la información en los contratos de prestación de servicios de manera específica.</p>
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	<p>En la página web de la Entidad, dentro del botón de transparencia y respecto a la documentación del proceso Gestión de Tecnologías de la Información y las Comunicaciones, se cuenta con el plan de capacitación y sensibilización de seguridad de la información de 2022 en el siguiente vínculo: https://culturarecreacionydeporte.gov.co/sites/default/files/2023-04/got-pn-01_plan_de_capacitacion_sensibilizacion_y_comunicacion_de_seguridad_de_la_informacion.pdf</p> <p>De acuerdo con lo mencionado, la oportunidad de mejora se presenta debido a que no se ha generado ni publicado el documento aprobado por la Alta Dirección para la vigencia 2023, por tal razón se sugiere actualizar la documentación y publicarla</p>

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		INFORME DE AUDITORIA INTERNA	
		FECHA: 18/05/2022	

		tanto en la página web como en la intranet.
21	Inventario de áreas de procesamiento de información y telecomunicaciones	No se relaciona soporte dentro de la información remitida al equipo auditor que refleje el inventario de áreas de procesamiento de información y telecomunicaciones. De acuerdo con la anotación generada en la matriz entregada por la OTI, este tema se debe solicitar a Infraestructura.
22	Diagrama de red de alto nivel o arquitectura de TI.	No se relaciona soporte dentro de la información remitida al equipo auditor. De acuerdo con la anotación generada por el responsable de la entrega de información (oficial de seguridad) en la matriz, este tema se debe solicitar a Infraestructura.
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad	En la matriz soporte que remite la OTI, no se remite evidencia de este aspecto, mencionando que <i>"No se conoce de la existencia del documento Solicitado."</i> Para tal fin se sugiere generar el documento asociado.
25	Formato de acuerdo de transferencia de información	En la matriz soporte que remite la OTI, no se remite evidencia de este aspecto, mencionando que <i>"No se conoce de la existencia del documento Solicitado."</i> Para tal fin se sugiere generar el documento asociado.
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	Frente a este aspecto, es mencionado por parte de la OTI en los comentarios de la matriz soporte la siguiente evidencia: Listado de Inventario de proveedores en proceso de levantamiento. Sin embargo, no se relaciona vínculo o adjunto donde se remita dicha información. Por tal motivo, se informa la oportunidad de mejora, a lo que se recomienda que la OTI genere el documento asociado y se mantenga actualizado a lo largo de cada vigencia.
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	Para este aspecto la OTI relaciona, dentro de la matriz soporte el Manual de políticas de seguridad y Privacidad de la información de la Secretaría de Cultura, Recreación y Deporte y al revisar dicho documento, en referencia al tema de indicadores del MSPI, se describe que se deben definir e implementar indicadores de Seguridad y privacidad de la información. Lo anterior indica que no se han generado indicadores tal como lo menciona este numeral. Por tal motivo se presenta la oportunidad de mejora, donde nos permitimos sugerir la construcción de indicadores enfocados en el tema

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

		de MSPI para la entidad y proceder con su correspondiente medición y monitoreo.
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	No se evidencia o relaciona por parte de la OTI el soporte respecto al cumplimiento de este numeral, para lo cual, desde la OCI, sugerimos sea construido y aprobado por la Alta Dirección para la presente vigencia.

Tabla N°7 Elaboración propia Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica – Hoja LEVANTAMIENTO DE INFO, suministrado por la OTI en agosto de 2023.

De acuerdo con los resultados expuestos en el cuadro anterior, se obtienen las siguientes oportunidades de mejora:

Oportunidad de mejora N°1: Falta de aprobación de documento de autoevaluación por parte de la Alta Dirección.

Oportunidad de mejora N°2: Falta de aprobación con el resultado de la herramienta de encuesta de diagnóstico de seguridad y privacidad de la información, por parte de la Alta Dirección.

Oportunidad de mejora N°3: Falta de aprobación de documento con la estratificación de la Entidad, por parte de la Alta Dirección.

Oportunidad de mejora N°4: Inexistencia de procedimiento oficial para control documental del MSPI en la entidad.

Oportunidad de mejora N°5: Debilidades respecto a los acuerdos contractuales (con contratistas) donde se establecen responsabilidades de las partes en referencia a seguridad de la información.

Oportunidad de mejora N°6: Inexistencia de plan de capacitación y sensibilización de seguridad de la información para la vigencia 2023, aprobado por la Alta Dirección.

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* : Radicado: RAD_S Fecha: F_RAD_S
		VERSIÓN: 01	
	INFORME DE AUDITORIA INTERNA	FECHA: 18/05/2022	

Oportunidad de mejora N°7: Falta de soporte con el Inventario de áreas de procesamiento de información y telecomunicaciones.

Oportunidad de mejora N°8: Falta de soporte con el diagrama de red de alto nivel o arquitectura de TI.

Oportunidad de mejora N°9: Falta de Inventario de partes externas o terceros a los que se transfiere información de la entidad.

Oportunidad de mejora N°10: Falta de Formato de acuerdo de transferencia de información.

Oportunidad de mejora N°11: Inexistencia de Indicadores oficiales de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.

Oportunidad de mejora N°12: Falta de Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.

5.5. **Ciberseguridad:**

Continuando con el proceso de seguimiento, el equipo auditor procedió a evaluar, dentro del instrumento de identificación de la línea base de seguridad administrativa y técnica, la hoja denominada **Ciber**, en la cual se observan ítems o requisitos valorados y/o calificados por la entidad con valor **CERO**, es decir, que no se han gestionado por parte de la Entidad o tienen un avance mínimo, los cuales se presentan a continuación:

REQUISITO CIBER
<p>La detección de actividades anómalas se realiza oportunamente y se entiende el impacto potencial de los eventos:</p> <ol style="list-style-type: none"> 1) Se establece y gestiona una línea base de las operaciones de red, los flujos de datos esperados para usuarios y sistemas. 2) Se agregan y correlacionan datos de eventos de múltiples fuentes y sensores. 3) Se determina el impacto de los eventos 4) Se han establecido los umbrales de alerta de los incidentes.
<p>Las actividades de restauración son coordinadas con las partes internas y externas, como los centros de coordinación, proveedores de servicios de Internet, los dueños de los sistemas atacados, las víctimas, otros CSIRT, y proveedores.:</p> <ol style="list-style-type: none"> 1) Se gestionan las comunicaciones hacia el público. 2) Se procura la no afectación de la reputación o la reparación de la misma. 3) Las actividades de recuperación son comunicadas a las partes interesadas internas y a los grupos de gerentes y directores.
<p>Las estrategias de respuesta se actualizan.</p>

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

Los planes de recuperación y los procesos son mejorados incorporando las lecciones aprendidas para actividades futuras:

- 1) Los planes de recuperación incorporan las lecciones aprendidas.
- 2) Las estrategias de recuperación son actualizadas.

Los sistemas de información y los activos son monitoreados a intervalos discretos para identificar los eventos de ciberseguridad y verificar la efectividad de las medidas de protección:

- 1) La red es monitoreada para detectar eventos potenciales de ciberseguridad.
- 2) El ambiente físico es monitoreados para detectar eventos potenciales de ciberseguridad.
- 3) Se monitorea en búsqueda de eventos como personal no autorizado, u otros eventos relacionados con conexiones, dispositivos y software.

Tabla N°8 Elaboración propia Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica – Hoja CIBER, suministrado por la OTI en agosto de 2023.

Por lo anterior, se presenta la siguiente oportunidad de mejora:

Oportunidad de mejora N°13: Aspectos relacionados con ciberseguridad con calificación 0 dentro de la entidad.

Una vez sustentado lo anterior, por parte de esta Oficina se recomienda avanzar en la planeación y ejecución de las actividades necesarias para la atención de los requisitos mencionados, con el fin de fortalecer la ciberseguridad y aportar al aumento del grado en el nivel de madurez de la entidad, de acuerdo con lo definido por el Instituto Nacional de Estándares y Tecnología NIST.

Finalmente, se reporta que el componente de Ciberseguridad tiene un porcentaje de avance total del 55,24%.

6. CONCLUSIONES

La incorporación de la seguridad de la información a los procesos, trámites, servicios, sistemas de información, infraestructura y a los activos de información es el derrotero que determina el Gobierno Nacional a través de la iniciativa de Gobierno Digital y, específicamente, a través de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual tiene como premisa la preservación de los 3 pilares de seguridad de la información titulados: confidencialidad, integridad y disponibilidad.

Alineado con lo anterior, se reconocen las actividades y estrategias desarrolladas por la Secretaría en cabeza, principalmente, de la Oficina de Tecnologías de la Información, quienes han demostrado un sólido compromiso, apuntando al aumento del nivel de madurez y el cumplimiento de los lineamientos establecidos por el MINTIC para el modelo en las

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

entidades públicas. Complementariamente, se resalta la documentación que, a través de las últimas vigencias, se ha estructurado y construido, observando la alineación con los procesos y procedimientos vigentes en el sistema integrado de gestión y en sí con la misión, visión y las metas institucionales.

Cabe resaltar que existen aspectos, descritos en el presente documento, que requieren una intervención y que son susceptibles de mejora, dentro de los cuales se mencionan: actualización de activos de información, gestión de riesgos de seguridad digital, optimización de la documentación del sistema, indicadores y disminución de la brecha respecto al Anexo A de la ISO 27001.

7. RECOMENDACIONES

- Establecer un proceso de revisión y monitoreo para asegurar el cumplimiento de los lineamientos nacionales en materia de seguridad y privacidad de la información.
- Fortalecer la información explicativa y la evidencia documental que se presenta por parte de la entidad en referencia a cada requisito descrito en el instrumento de identificación de línea base compartido por el MINTIC, toda vez que se encontraron algunas debilidades o ausencias de soportes que daban cuenta del cumplimiento de los requisitos.
- Generar los planes de acción necesarios para iniciar la atención de los requisitos con calificación cero, principalmente los relacionados con Ciberseguridad.
- Continuar e intensificar, a nivel institucional, la cultura, conciencia y apropiación en materia de seguridad de la información, por medio de estrategias y campañas donde a todo el personal se refuercen los conceptos y la aplicación de los controles, para así evitar la materialización de riesgos y la explotación de las vulnerabilidades, por parte de externos, que pretendan afectar la ejecución de la misionalidad.
- Optimizar los procesos y adicionar nuevos ítems derivados de la evaluación de riesgos que continuamente se realiza, incluyendo una revisión más frecuente y detallada de las amenazas potenciales, alineadas con la realidad operativa de la Secretaría.
- Crear nuevos controles encaminados a la protección de datos sensibles o tipificados como críticos en la entidad, tales como datos personales de ciudadanos, empleados y contratistas.

	PROCESO DE SEGUIMIENTO Y EVALUACIÓN A LA GESTIÓN	CÓDIGO: SEG-PR-02- FR-03	*RAD_S* Radicado: RAD_S Fecha: F_RAD_S
	INFORME DE AUDITORIA INTERNA	VERSIÓN: 01	
		FECHA: 18/05/2022	

- Tener en cuenta la documentación generada por el MinTIC a través de la página web de Gobierno Digital publicada en el siguiente vínculo <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/> . Por medio de esta documentación se orienta y se da línea a las entidades públicas de las actividades que se deben desarrollar en el marco del MSPI que, al ser tenidas en cuenta, garantizan la idoneidad y eficacia de las estrategias y actividades a realizar, apuntando a una acertada toma de decisiones.

8. PLAN DE MEJORAMIENTO

Como aspecto final, derivado del ejercicio de seguimiento realizado por la Oficina de Control Interno y con el fin de mitigar los riesgos asociados, se solicita informar a la Oficina Asesora de Planeación, dentro de los diez (10) días hábiles posteriores a la comunicación del informe final de auditoría, las acciones correctivas o de mejora a implementar, en cumplimiento del Procedimiento para la mejora, lo anterior con el fin de fortalecer el cumplimiento de los lineamientos nacionales en materia de seguridad y privacidad de la información y ciberseguridad.

9. FIRMAS

Elaboró

Aprobó

DIEGO ALEXANDER URAZAN FRANCO
Contratista

OMAR URREA ROMERO
Jefe Oficina Control Interno