# COMUNICACIÓN INTERNA

Bogotá D.C., martes 27 de diciembre de 2022

PARA:

Catalina Valencia Tobón
Secretaria de Cultura, Recreación y Deporte

Carlos Maroni Magaldi Manotas
Jefe Oficina de Tecnologías de la Información

Carlos Alfonso Gaitán Sánchez
Jefe Oficina Asesora de Planeación

Yaneth Suárez Acero
Subsecretaria de Gobernanza

Henry Samuel Murrain Knudson
Subsecretario de Cultura Ciudadana y Gestión del Conocimiento

Adriana María Cruz Rivera
Directora de Gestión Corporativa y Relación con la Comunidad

Jaime Andrés Tenorio Tascón
Director de Arte y Patrimonio

Rafael Eduardo Tamayo Franco
Director de Lectura y Bibliotecas

Juan Manuel Vargas Ayala
Jefe Oficina Asesora Jurídica

Carolina Ruíz Caicedo
Jefe Oficina Asesora de Comunicaciones

DE:

Omar Urrea Romero
Jefe Oficina de Control Interno

ASUNTO:

Informe Final de Auditoría al Modelo de Privacidad y Seguridad de la Información (MSPI) de la Secretaría.

Estimados integrantes del Comité de Coordinación de Control Interno,

De manera atenta informo que, en desarrollo del Plan Anual de Auditoría de la Secretaría (SCRD) para la vigencia 2022, se ha concluido el trabajo de Auditoría Interna referente a la Evaluación al Modelo de Privacidad y Seguridad de la Información – MPSI en la SCRD.

Como resultado del trabajo se resaltan **un (1) Cumplimento** a razón de los criterios de auditoría y elementos demostrados por los auditados; **un (1) Incumplimiento** y **quince (15) Oportunidades de Mejora** que en detalle se podrán analizar en el Informe anexo, resumidos en la siguiente tabla:

| TIPO DE RESULTADO | CANTIDAD | REFERENCIACIÓN |
|---|---|---|
| Fortalezas | 0 | |
| Cumplimientos | 1 | 5.17 |
| Incumplimientos | 1 | 5.16 |
| Oportunidades de Mejora | 15 | 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, 5.12, 5.13, 5.14, 5.15. |
| **TOTAL:** | 17 | |

En relación con la tabla anterior, el Modelo de Seguridad y Privacidad de la Información en la Secretaría se encontró en un avance del 30%, resumido en cuatro (4) fases: planificación, implementación, evaluación de desempeño y mejora continua, 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% |

*Ilustración 3. Captura de pantalla del porcentaje de avance evidenciado durante el desarrollo de la auditoría.*

La evaluación del MSPI indicó que resulta importante avanzar en la atención de las siguientes actividades descritas y desarrolladas a lo largo del informe de auditoría:

1. Formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en la Secretaría. Se recomienda que dicho responsable sea trasversal a la entidad y cercano a la alta dirección, conforme a las disposiciones vigentes en la citada materia por el MSPI.

2. Priorizar y finalizar las actividades pendientes por desarrollar en la fase de “Planificación” del modelo para llevar a buen término la implementación y las demás etapas del Modelo de Seguridad y Privacidad de la Información en la SCRD.

3. Finalizar el levantamiento de activos de información en la SCRD, para luego, concluir con la evaluación y valoración de los riesgos de Seguridad y Privacidad de la Información de la totalidad de activos de información identificados en la Secretaría. Estas actividades serán la base para la implementación de los controles que ayudarán a mitigar los riesgos en la fase No. 3 de operación y/o implementación, en la cual serán desarrollados. La gestión de riesgos deberá ser dinámica y sistemática en cada uno de los procesos de la SCRD.

4. Formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI de la SCRD. 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 los que se describan los lineamientos que se deberán ejecutar para gestionar la Seguridad de la Información.

5. 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 los dispuesto en la fase 4 “Evaluación y desempeño”, con el objetivo de medir su desempeño y eficiencia.

6. 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, con el objetivo de dar cumplimiento a lo dispuesto en la fase 4 “Evaluación y desempeño” del MSPI.

Los anteriores resultados fueron expuestos en la reunión de cierre de auditoría realizada el pasado 23 de diciembre de 2022.

Finalmente, se solicita a los líderes de este proceso y a las demás áreas involucradas (particularmente Oficina de Planeación y Oficina de Tecnologías de la Información), en cumplimiento del proceso de mejora y con el apoyo de la Oficina Asesora de Planeación, que en los siguientes diez (10) días hábiles posteriores a la comunicación del presente informe, se establezca el plan de mejora con las acciones correctivas y de mejora a implementar.

Cualquier inquietud, con gusto estamos atentos.

Atentamente,

Omar Urrea Romero
Jefe Oficina de Control Interno

Anexo: Informe detallado de auditoría.

**Documento 20221400541903 firmado electrónicamente por:**

**Omar Urrea Romero**, Jefe Oficina de Control Interno, Oficina de Control Interno,
Fecha firma: 27-12-2022 08:48:05

edédd05ad861220786d8141f2569863d8e48b9e50c6b6f37ae12b0d87feab3ce

# TABLA DE CONTENIDO

## 1. DESCRIPCIÓN GENERAL

| | |
|---|---|
| **NOMBRE DE LA AUDITORÍA** | Modelo de Privacidad y Seguridad de la Información – MPSI en la Secretaría de Cultura, Recreación y Deporte de Bogotá D.C. |
| **TIPO DE AUDITORÍA** | Auditoría interna basada en riesgos. |
| **UNIDAD (ES) AUDITABLES** | GOT-CP GESTIÓN OPERATIVA DE TI |
| **RESPONSABLE (S)** | Líderes de Proceso.<br>Jefe de la Oficina de Tecnologías de la Información.<br>Jefe Oficina Asesora de Planeación.<br>Comité de Gestión y Desempeño.<br>Comité de Coordinación de Control Interno. |
| **OBJETIVO** | Verificar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Secretaría Distrital de Cultura, Recreación y Deporte - SCRD, en concordancia con los lineamientos de las Políticas Gobierno Digital y Seguridad Digital del Modelo Integrado de Planeación y Gestión (MIPG) |
| **ALCANCE** | Elementos de control, documentación e información asociadas con el proceso GOT-CP V1, y aquellos vigentes de la versión 8 del Mapa de Procesos, con el propósito de determinar fortalezas, debilidades y oportunidades de mejora al MPSI en la SCRD. El periodo de evaluación cubrirá desde septiembre 01 de 2021 hasta septiembre 30 de 2022. |
| **PERIODO DE EJECUCIÓN** | Octubre 01 al 03 de diciembre de 2022. |
| **EQUIPO AUDITOR**[1] | Omar Urrea, Auditor, Auditor Líder, jefe Oficina de Control Interno<br>Marco Ramiro Marín Buitrago, Auditor interno principal.<br>Andrés Pabón Salamanca, Auditor interno observador. |

1 Escriba los nombres del Equipo Auditor, el acrónimo correspondiente, así como el rol a desempeñar (Auditor Líder, Auditor Interno, Observador, y/o Experto Técnico)

## 2. CRITERIOS DE AUDITORÍA

- Proyecto de inversión 7646 denominado "Fortalecimiento a la gestión, la innovación tecnológica y la comunicación pública de la Secretaría de Cultura, Recreación y Deporte de Bogotá".
- 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.
- 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.
- Acta No. 03 del 23 de mayo de 2022 en el cual se ajustó el Plan Anual de Auditoría de la Secretaría a las necesidades de aseguramiento y de los resultados de la aplicación al Formulario Único Reporte de Avances de la Gestión (FURAG) del MIPG en la SCRD, incluyendo la verificación al Sistema de Gestión de seguridad de la información y Seguridad Digital bajo el MSPI.
- Lineamientos contenidos en el Manual Operativo del MIPG y Consejo para la Gestión y Desempeño Institucional (Versión 4 marzo de 2021), referentes a la Política Gobierno Digital y Política de Seguridad Digital.

## 3. METODOLOGÍA

Durante el desarrollo de la auditoría, se hicieron entrevistas, se revisaron documentos, procesos y procedimientos, en general, se obtuvo la información suficiente y relevante para el desarrollo del siguiente informe:

- **El Modelo de Seguridad y Privacidad de la Información[2] – MSPI**

Es un mecanismo elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), basado en normas internacionales[3], en el que se definen los lineamientos que deberán seguir los sujetos obligados[4] en la implementación de la

2 *Resolución 500 del 10 de marzo de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.*

3 *El modelo se basa en el estándar ISO 27001:2013 y en otros como las del Instituto Nacional de Estándares y Tecnología, por sus siglas del inglés (NIST).*

4 *Definidos en la ley 1712 de 2014.*

estrategia de la política de seguridad digital[5] colombiana. El MSPI tiene como objetivo el formalizar al interior de las entidades el Sistema de Gestión de Seguridad y Privacidad de la información – SGSI[6], el cual, se deberá desarrollar en cinco (5) fases a través del ciclo de Deming o PHVA (Planear, Hacer, Verificar y Actuar):

- Fase 1: Diagnóstico
- Fase 2: Planificación
- Fase 3: Operación y/o implementación
- Fase 4: Evaluación de desempeño
- Fase 5: Mejora continua

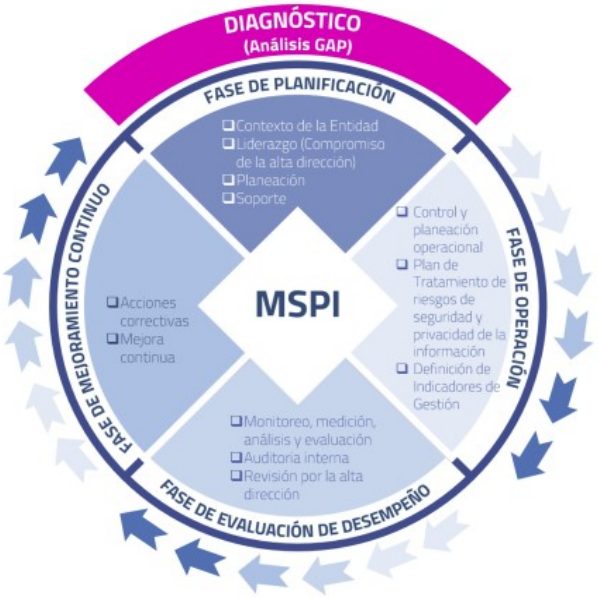



*Ilustración 1. Ciclo PHVA propuesto en el documento maestro del MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)*

La información considerada como sensible o de valor, deberá ser identificada y reconocida como un activo de información. El SGSI tiene como propósito la identificación y protección de la información[7] que la Secretaría de Cultura, Recreación y Deporte - SCRD así considere, que podría tener relación con la propiedad intelectual, los datos financieros, los registros legales, comerciales y operativos, relacionados con empleados, proveedores y grupos de interés.

---

5 *https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf*

6 *Pág. No. 6 del documento maestro del MSPI.*
*https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf*

7 *Hace referencia a los activos de información que se identifiquen en la SCRD y la protección de los riesgos asociados a la Integridad, Confidencialidad y Disponibilidad.*

Los tipos de riesgos[8] a los que se enfrenta esta información sensible se agrupan en tres categorías:

- Confidencialidad es la propiedad de la información que garantizará el nivel de acceso que tendrá una entidad o persona sobre un activo de información, con el objeto de prevenir su divulgación no autorizada.
- Integridad es la propiedad de la información que garantizará la exactitud de los datos en tránsito o en reposo, asegurando que el contenido no cambiará ya sea de manera accidental o intencionada.
- Disponibilidad, es la propiedad de la información que garantizará el acceso oportuno a los datos o recursos por parte de entidades o personas autorizadas.

En relación con lo anterior, los tipos de riesgos deberán gestionarse de acuerdo con el estado de la información, debido a que no serán los mismos riesgos o niveles de riesgos cuando estos se encuentran en alguno de los siguientes:

- En tránsito, cuando los datos se mueven a través de las redes de comunicaciones o sistemas de información.
- En reposo, cuando los datos se encuentran almacenados, no son accedidos o usados, pero se deberán preservar en medios lógicos o físicos.
- En proceso, cuando los datos se encuentran en uso o gestionados por entidades.

El MSPI propuesto por el MINTIC se encuentra alineado con estándares Internacionales, como la ISO/IEC 27001:2013, el marco de ciberseguridad del NIST[9], la ISO/IEC 31000, con el Marco de Referencia de Arquitectura[10] de TI, el Modelo Integrado de Planeación y Gestión (MIPG[11]), la Guía[12] de Administración de Riesgos y el Diseño de Controles en entidades Públicas, la ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública (ley 1581 de 2012), entre otras.

- **El modelo de madurez**

8 *Los riesgos de Seguridad y Privacidad de la Información se encuentran establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020.*

9 *Acrónico del Instituto Nacional de Estándares y Tecnología (National Institute of Standars and Technology, en inglés), https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist*

10 *https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8118.html*

11 *https://www.funcionpublica.gov.co/web/mipg*

12 *https://www.mincit.gov.co/temas-interes/documentos/guia-para-la-administracion-del-riesgo-y-el-diseno.aspx*

De acuerdo con lo descrito en el capítulo 9[13] del documento denominado “Modelo de Seguridad y Privacidad de la Información” propuesto como parte del MSPI del MINTIC, el modelo de madurez “busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en la entidad”. La herramienta de autodiagnóstico propuesta por el MINTIC pretende identificar el nivel de madurez actual del MSPI, midiendo la brecha entre el nivel actual y el optimizado, de acuerdo con la siguiente escala:

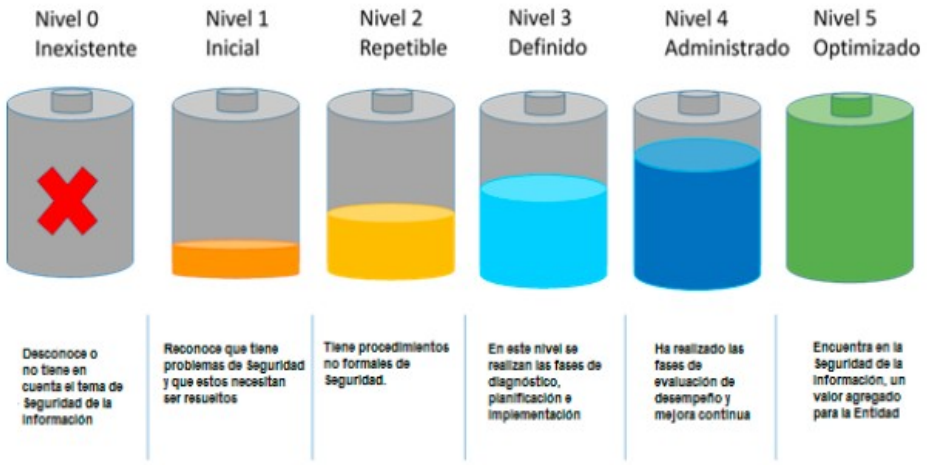



*Ilustración 2 Niveles de madurez propuestos en el documento denominado “Modelo de Seguridad y Privacidad de la Información” propuesto como parte del MSPI del MINTIC*

A continuación, se describen cada una de las etapas[14] propuestas por el MINTIC a través del documento[15] maestro del MSPI y lo evidenciado durante el desarrollo de la auditoría en la Secretaría de Cultura, Recreación y Deporte - SCRD:

## 3.1. Fase 1: Diagnóstico

La fase de diagnóstico tiene como objetivo identificar el estado actual del MSPI en la SCRD a través de un análisis GAP[16] o de brechas, que deberá desarrollarse a través de la herramienta de autodiagnóstico propuesta por el MINTIC. Durante el desarrollo de la auditoría, la SCRD compartió el documento denominado “SCRD MSPI MINTIC JULIO

13 *https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf*

14 *Será de obligatorio cumplimiento para los sujetos obligados en la ley 1712 de 2014.*

15 *Documento Maestro del Modelo de Seguridad y Privacidad de la Información, link: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf*

16 *GAP o Destacado, mejorable, normal, por sus siglás del inglés Good, Average, Poor, haciendo referencia a una empresa. Es un análisis para identificar la brecha de lo actual versus el nivel deseado.*

2022.xlsx" en el cual se evidencia el cumplimiento de esta actividad. De relevante, se encontró un 30% de avance en la implementación del MPSI en la SCRD frente a un 34% que se encontró al inicio de la auditoría:

| Año | AVANCE PHVA | | |
|---|---|---|---|
| | COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
| 2022 | Planificación | 26% | 40% |
| | Implementación | 5% | 20% |
| | Evaluación de desempeño | 3% | 20% |
| | Mejora continua | 0% | 20% |
| TOTAL | | 34% | 100% |

*Ilustración 2. Captura de pantalla del porcentaje de avance encontrado en el documento denominado "SCRD MSPI MINTIC JULIO 2022.xlsx"*

Durante el desarrollo de la auditoría, se hizo la evaluación y se evidenció un avance del 30%. La fase de "Planificación" tuvo una leve reducción y las demás permanecieron estables. Los resultados de estos porcentajes serán detallados a lo largo del informe:

| 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% |

*Ilustración 3. Captura de pantalla del porcentaje de avance evidenciado durante el desarrollo de la auditoría.*

La herramienta de diagnóstico propuesta por el MINTIC es dinámica, lo que indica que, a medida que se avance en las fases de planificación, operación y/o implementación, evaluación de desempeño y mejoramiento continuo, se deberán actualizar a partir del análisis y gestión de los riesgos de seguridad de la información, la efectividad de los controles propuestos para mitigarlos, la medición y análisis de esos controles, la revisión de los incidentes de seguridad, entre otros, serán parte de la mejora continua.

## 3.2. Fase 2: Planificación

Durante el desarrollo de la auditoría se evidenció un 20% de avance en esta fase.

| COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
|---|---|---|
| **Planificación** | **20%** | **40%** |

*Ilustración 3. Porcentaje de avance encontrado en la etapa de "Planificación".*

Durante esta fase, se deberán establecer las necesidades y los objetivos del MSPI, los cuales, deberán reflejar el alcance y los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) que se pretende implementar en la SCRD. Sobre el particular, durante el desarrollo de la auditoría, se evidenció el documento denominado "Plan de seguridad de la información (GOT-PN-02)" publicado el 31 de enero de 2022, en el cual, la SCRD propuso un periodo de 11[17] meses para dar alcance al objetivo propuesto *"...una hoja de ruta y las actividades que hacen parte de la implementación…"* del MSPI en la entidad. Sin embargo, durante el desarrollo de la auditoría se evidenció que algunas de estas actividades no han finalizado, se encuentran en desarrollo o tienen fechas de culminación para el año 2023, más allá de la fecha propuesta inicialmente.

El siguiente es el esquema propuesto por el MINTIC en durante esta fase:

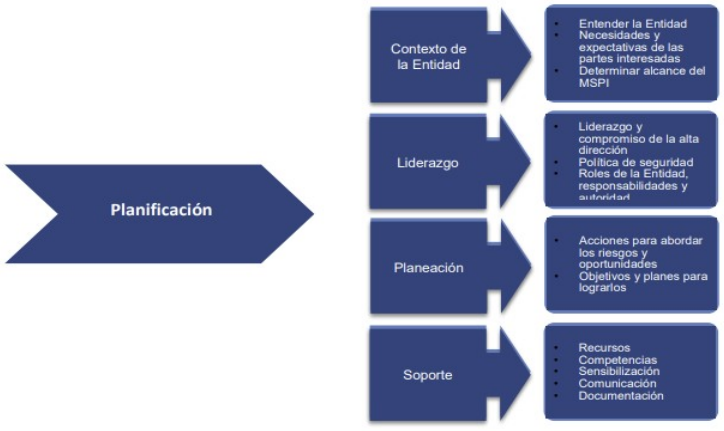



*Ilustración 4. Captura de pantalla del modelo de la fase de planificación propuesto por el MINTIC*

17 *Los 11 meses se encuentran definidos en la página 4 del documento "Plan de Seguridad de la Información SCRD", entre el 31 de enero y el 31 de diciembre de 2022.*

### 3.2.1. Contexto de la SCRD

El contexto[18] de la organización se encontró desarrollado en el apartado "Modelo Integrado de Planeación y Gestión (MIPG)[19]" de la SCRD, donde se evidenció un grupo de documentos formalizados y relacionados con el contexto de la organización. Se relacionan algunos documentos:

- Documento "FT-01-CP-DES v4 Conocimiento y contexto de la Organización - PEI 2021"
    - Plan estratégico Institucional 2020-2024
    - Análisis de Contexto Sector Cultura, Recreación y Deporte 2021
    - Plan Estratégico Sectorial (PES) 2021

- Documento "FT-02-CP-DES v3 Matriz de Partes Interesadas 22/10/2020
- FT-01-PR-DES-15 v3 Matriz de Planificación de cambios

El documento denominado "Análisis de Contexto Sector Cultura, Recreación y Deporte 2021", se encontró asociado al Plan Estratégico Institucional de las vigencias 2020/2024, fue desarrollado a partir de un análisis PESTEL[20], donde se involucraron las variables políticas, económicas, sociales, ambientales, legales y tecnológicas. Sin embargo, en el documento de contexto no se abordaron los asuntos relacionados con la Seguridad y Privacidad de la Información como parte del diagnóstico del MSPI en la SCRD. En este análisis se deberían considerar los objetivos propuestos en el SGSI de la SCRD, la madurez de los procesos, los potenciales riesgos y los controles propuestos a los activos de información identificados.

El documento denominado "Documento FT-02-CP-DES v3 Matriz de Partes Interesadas 22/10/2020" contiene la "matriz_planificacion_de_cambios_v3_0.xlsx", la cual, desarrolló las "necesidades y expectativas de las partes interesadas". Sin embargo, en la matriz no se encontró el relacionado con la dirección de "Lectura y Bibliotecas":

18 *El contexto de la organización se encuentra desarrollado en la cláusula número 4.0 de la norma ISO/IEC 27001:2013*

19 *https://intranet.culturarecreacionydeporte.gov.co/sig*

20 *PESTEL: Análisis de mercado donde se analizan factores Políticos, Económicos, Sociales, Tecnológicos, Ecológicos y Legales.*

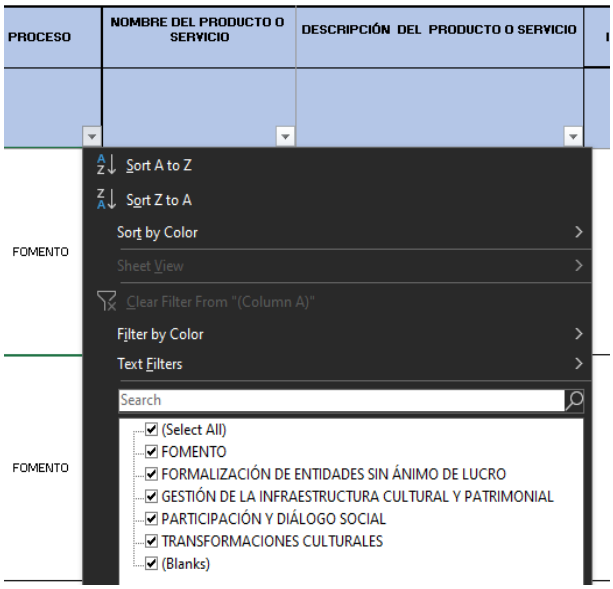



*Ilustración 5. Se evidencia filtro en el documento denominado "matriz_planificacion_de_cambios_v3_0.xlsx"*

### 3.2.1.1. Alcance del MSPI

Los objetivos y el alcance del MSPI se deberán reflejar en los propuestos para el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSI que se pretende implementar en la SCRD. Sin embargo, estos objetivos no se evidenciaron durante el desarrollo de la auditoría.

Los objetivos, el alcance y los límites del SGSI se deberán implementar en esta fase como lo indica el numeral "8.2 Fase de planificación" del documento denominado "Modelo de seguridad y Privacidad de la Información[21]" propuesto por el MINTIC, y lo descrito en la cláusula 1.0 del estándar ISO 27001:2013. En estos objetivos se deberían integrar los procesos misionales de la SCRD, ubicaciones físicas, terceros (operadores) relacionados, infraestructura tecnológica propia y la administrada por terceros que tienen incidencia directa con la SCRD. Proponerse objetivos ambiciosos podría llevar el MSPI a escenarios de certificación de la norma, que sería el siguiente nivel a lo indicado por el MINTIC.

### 3.2.2. Liderazgo

21 https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

El Liderazgo[22] es un conjunto de actividades que desde la dirección estratégica se implementan como apoyo a la implementación del Modelo de Seguridad y Privacidad de la Información en la SCRD. A continuación, se describirán, las principales actividades evidenciadas durante el desarrollo de la auditoría:

### 3.2.2.1. Liderazgo y Compromiso

En 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)” se evidenció el liderazgo y compromiso de la dirección y en las actividades descritas a lo largo de este reporte y en el proyecto de inversión 7646 denominado "Fortalecimiento a la gestión, la innovación tecnológica y la comunicación pública de la Secretaría de Cultura, Recreación y Deporte de Bogotá".

### 3.2.2.2. Política de seguridad y privacidad de la información.

Durante el desarrollo de la auditoría se evidenció que la SCRD cuenta con una “Política General de Seguridad de la Información (GOT-PL-01)”, publicada el 31 de enero de 2022 y aprobada por la dirección, dando cumplimiento con los requisitos propuestos por el MSPI y la ISO 27001:2013.

Así mismo, durante el desarrollo de la auditoría se evidenció el documento denominado “Manual de Políticas de Seguridad y Privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte (GOT-MN-01)[23]”, en el cual, se evidenció un conjunto de 26 políticas aprobadas por el Coordinador de GIT de Infraestructura y Sistemas de Información:

| | |
|---|---|
| Política de control de acceso | MSPI - (Pág. 31) |
| Política de gestión de activos | MSPI - (Pág. 22) |
| Política de clasificación y manejo de activos de información. | MSPI - (Pág. 28) |
| Política de uso aceptable de activos de información | MSPI - (Pág. 23) |
| Política de escritorio y pantalla limpia. | MSPI - (Pág. 40) |
| Política de Teletrabajo y dispositivos móviles | MSPI - (Pág. 18) |
| Política de continuidad de negocio. | MSPI - (Pág. 50) |
| Política contra código maliciosos | MSPI - (Pág. 41) |

22 *Se encuentra descrito en la cláusula No. 5 del estándar ISO 27001:2013*

23 *Cumplimiento a lo dispuesto en el MSPI del MINTIC.*

| | |
|---|---|
| Política de gestión de cambios | MSPI - (Pág. 41 y 47) |
| Política de seguridad en la relación con los proveedores | MSPI - (Pág. 46) |
| Política de registro y seguimiento | MSPI - (Pág. 42) |
| Política de gestión de seguridad en la red | MSPI - (Pág. 43) |
| Política de transferencia de información | MSPI - (Pág. 44) |
| Política de desarrollo seguro | MSPI - (Pág. 47) |
| Política de seguridad física y del entorno | MSPI - (Pág. 38) |
| Política de criptografía | MSPI - (Pág. 37) |
| Política de gestión de incidentes de seguridad de la información | MSPI - (Pág. 49) |
| Política de cumplimiento | MSPI – (Pág. 10, 11) |
| Política en la gestión de proyectos | MSPI – (Pág. 17) |
| Política en el recurso humano | MSPI – (Pág. 20) |
| Política en la seguridad de las operaciones | MSPI – (Pág. 41) |
| Política de copia de seguridad | MSPI – (Pág. 42) |
| Política en la seguridad en las comunicaciones | MSPI – (Pág. 43) |
| Política de Adquisición, Desarrollo y Mantenimiento de Sistemas | MSPI – (Pág. 45) |

*Tabla 1. Relación de políticas encontradas en el "Manual de Políticas de Seguridad y Privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte (GOT-MN-01)"*

Durante el desarrollo de la auditoría no se evidenciaron los procedimientos[24], guías o instructivos asociados al conjunto de políticas encontradas en el "Manual de Políticas de Seguridad y Privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte (GOT-MN-01) que se relacionaron anteriormente, y que, de acuerdo con el MSPI[25], son necesarios para desarrollar la fase de implementación del MSPI en la SCRD.

Algunos procesos, procedimientos y guías se encontraron en la "intranet" o "Cultunet" [26] de la SCRD, sin embargo, resultó confuso para el desarrollo de la auditoría buscar y encontrar esos documentos relacionados con la Secretaría y, en general, con el MSPI, debido a que se encontraron dos ubicaciones diferentes:

- La primera, en la ruta: menú "MIPG", título "Documentación transitoria de los procesos V.8" Procesos de apoyo Gestión de TIC. En este sitio se encontraron procesos, procedimientos, manuales y formatos relacionados con TIC y algunos

24 *El MINTIC propone la "Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información" para el desarrollo de esta actividad, sin embargo, la SCRD podrá implementar la que mejor se ajuste a sus requerimientos.*

25 *Numeral "8.2 Fase de Planificación" del Modelo de Seguridad y Privacidad propuesto por el MINTIC, enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf*

26 *https://intranet.culturarecreacionydeporte.gov.co/pagina-principal*

relacionados con la Seguridad y Privacidad de la Información, los cuales fueron publicados en los años 2018 y 2019:

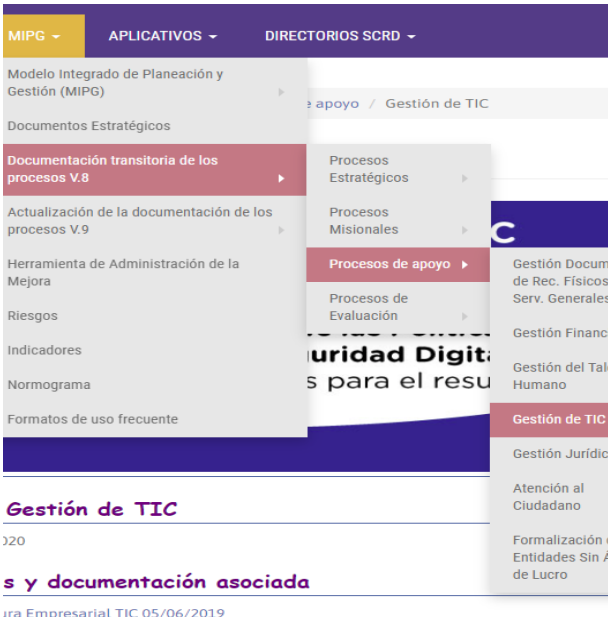



*Ilustración 6. Captura de pantalla de la ubicación en Cultunet, menú "MIPG", título "Documentación transitoria de los procesos V.8"  Procesos de apoyo  Gestión de TIC*

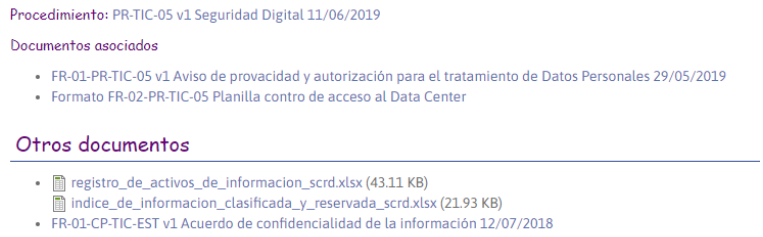



*Ilustración 7. Relación de documentos encontrados en la ubicación en Cultunet menú "MIPG", título "Documentación transitoria de los procesos V.8"  Procesos de apoyo  Gestión de TIC*

- La segunda, corresponde con la ubicación del menú "MIPG", título "Actualización de la documentación de los procesos V.9"  Procesos de apoyo  Gestión operativa de TI. En este sitio se encontró el proceso de Gestión Operativa de TI, la política de seguridad de la información, planes, manuales y otros documentos relacionados con la seguridad y privacidad de la información del año 2022:

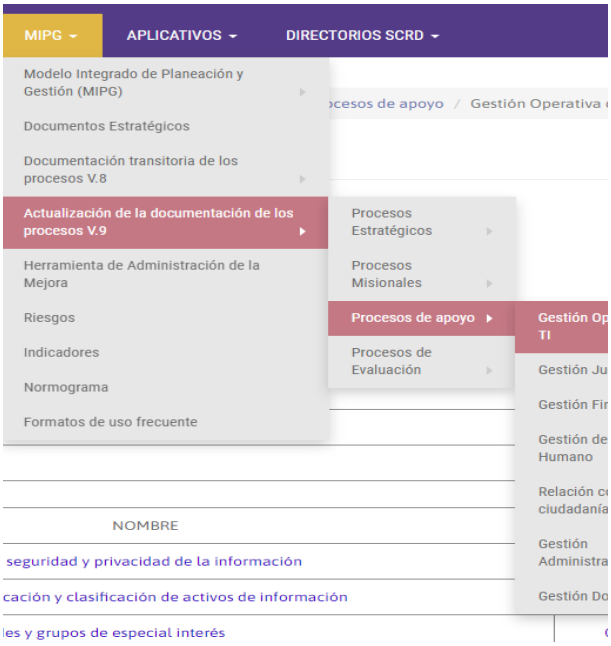
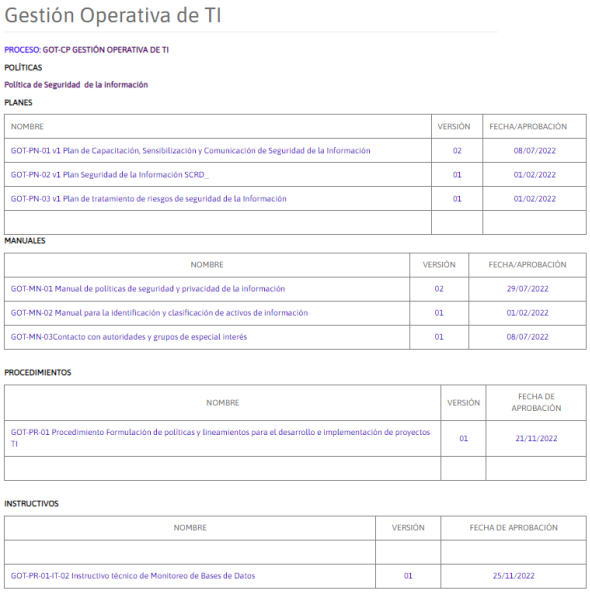



*Ilustración 8. Ubicación en la Cultunet menú "MIPG", título "Actualización de la documentación de los procesos V.9"  Procesos de apoyo  Gestión operativa de TI*



Gestión Operativa de TI

PROCESO: GOT-CP GESTIÓN OPERATIVA DE TI

POLÍTICAS

Política de Seguridad de la Información

PLANES

| NOMBRE | VERSIÓN | FECHA/APROBACIÓN |
|---|---|---|
| GOT-PN-01 v1 Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información | 02 | 08/07/2022 |
| GOT-PN-02 v1 Plan Seguridad de la Información SCRD_ | 01 | 01/02/2022 |
| GOT-PN-03 v1 Plan de tratamiento de riesgos de seguridad de la Información | 01 | 01/02/2022 |
| | | |

MANUALES

| NOMBRE | VERSIÓN | FECHA/APROBACIÓN |
|---|---|---|
| GOT-MN-01 Manual de políticas de seguridad y privacidad de la información | 02 | 29/07/2022 |
| GOT-MN-02 Manual para la identificación y clasificación de activos de información | 01 | 01/02/2022 |
| GOT-MN-03Contacto con autoridades y grupos de especial interés | 01 | 08/07/2022 |

PROCEDIMIENTOS

| NOMBRE | VERSIÓN | FECHA DE APROBACIÓN |
|---|---|---|
| GOT-PR-01 Procedimiento Formulación de políticas y lineamientos para el desarrollo e implementación de proyectos TI | 01 | 21/11/2022 |
| | | |

INSTRUCTIVOS

| NOMBRE | VERSIÓN | FECHA DE APROBACIÓN |
|---|---|---|
| | | |
| GOT-PR-01-IT-02 Instructivo técnico de Monitoreo de Bases de Datos | 01 | 25/11/2022 |

*Ilustración 9. Relación de documentos encontrados en la ubicación menú "MIPG", título "Actualización de la documentación de los procesos V.9"  Procesos de apoyo  Gestión operativa de TI*

### 3.2.2.3. Roles y responsabilidades

El Modelo de Seguridad y Privacidad de la Información – MSPI, propuesto por el MINTIC, indica que las "entidades deben definir internamente las responsabilidades"[27] en esta materia, designando a las personas apropiadas y con el propósito de articular las áreas de la entidad, los procesos, procedimientos, los roles y responsabilidades, necesarios para la adopción del MSPI en la SCRD.

Durante el desarrollo de la auditoría se evidenció que en el numeral "6. Organización de la seguridad de la información" del "Manual de Políticas de Seguridad y Privacidad de la Información de la Secretaría de Cultura, Recreación y Deporte (GOT-MN-01)", relaciona los responsables para la seguridad de la información de la SCRD. Así mismo, se evidenció que a través de la resolución 20 del 12 de enero de 2021, la SCRD modificó el "Manual específico de funciones y de competencias laborales" adicionando algunas funciones relacionadas con la "Seguridad y Privacidad de la Información" en la Secretaría, y asignando la responsabilidad de este rol al jefe de la Oficina de Tecnologías e Información (OTI)

Sin embargo, los numerales "3.2.1.4. Política de seguridad digital de MIPG[28]" y "7.2.3 Roles y responsabilidades[29]" del documento maestro del Modelo de Seguridad y Privacidad de la Información, 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[30]":

> De otro lado, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, 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. Para las entidades cabeza de sector, el Responsable de Seguridad Digital será el designado como enlace sectorial de seguridad digital.

*Ilustración 10. Captura de pantalla del numeral "3.2.1.4. Política de seguridad digital" de MIPG*

27 *Roles y responsabilidades del Modelo de Seguridad y Privacidad de la Información del MINITC, enlace: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237904_maestro_mspi.pdf*

28 *Enlace: https://www.funcionpublica.gov.co/documents/28587410/34112007/Manual+Operativo+MIPG.pdf/ce5461b4-97b7-be3b-b243-781bbd1575f3?t=1638367931337*

29 *Enlace: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf*

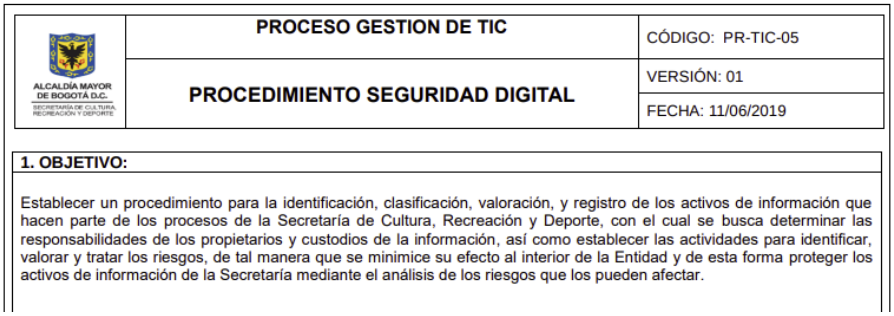
30 *El MINTIC propone la "Guía 4- Roles y responsabilidades" para desarrollar este ítem, sin embargo, la SCRD podrá incorporarla o no. Link: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150523_G4_Roles_responsabilidades.pdf*

### 3.2.3. Planeación

El Modelo de Seguridad y Privacidad de la Información - MSPI establece que, en esta etapa, se deberá realizar la identificación de los activos de información, sobre los cuales se deberá hacer la identificación, evaluación y tratamiento de los riesgos[31] de Seguridad y Privacidad de la Información de la SCRD.

Durante el desarrollo de la auditoría, se evidenció que la SCRD cuenta con una Política de Administración de Riesgos (DES-POL-01), un Proceso (DES-PR-09) y un Manual (DES-MN-04) de "Gestión de Riesgos de Seguridad de la Información", las cuales se encuentran alineadas con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5, definida por el Departamento Administrativo de la Función Pública (DAFP).

Así mismo, se evidenció que la SCRD cuenta con un manual para la identificación y clasificación de activos de información (GOT-MN-02), publicado el 1 de febrero de 2022 y con el que se evidencia la gestión de la identificación de activos en la Secretaría. Sin embargo, resultó confuso al encontrar un segundo documento con características similares al anterior, publicado el 11 de junio de 2019 en la "Cultunet" de la SCRD y denominado "Procedimiento de Seguridad Digital (PR-TIC-05)[32]", asociado al proceso de Gestión de TIC de la SCRD, en el que se describen las actividades que se deberán desarrollar en la "la identificación, clasificación, valoración, y registro de los activos de información que hacen parte de los procesos de la Secretaría de Cultura, Recreación y Deporte":



| ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE | **PROCESO GESTION DE TIC** | CÓDIGO: PR-TIC-05 |
|---|---|---|
| | **PROCEDIMIENTO SEGURIDAD DIGITAL** | VERSIÓN: 01 |
| | | FECHA: 11/06/2019 |

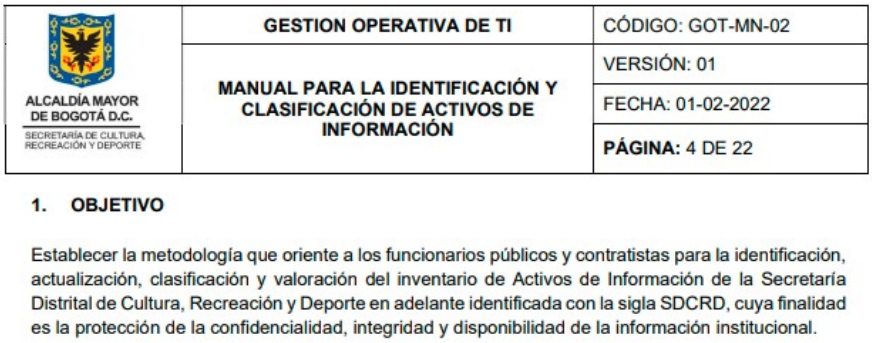
**1. OBJETIVO:**

Establecer un procedimiento para la identificación, clasificación, valoración, y registro de los activos de información que hacen parte de los procesos de la Secretaría de Cultura, Recreación y Deporte, con el cual se busca determinar las responsabilidades de los propietarios y custodios de la información, así como establecer las actividades para identificar, valorar y tratar los riesgos, de tal manera que se minimice su efecto al interior de la Entidad y de esta forma proteger los activos de información de la Secretaría mediante el análisis de los riesgos que los pueden afectar.

*Ilustración 11. Captura de pantalla del procedimiento publicado en la "Cultunet" denominado "Procedimiento de Seguridad Digital"*

31 *La planeación se encuentra desarrollada en la cláusula 6, del estándar ISO 27001:2013*

32 *https://intranet.culturarecreacionydeporte.gov.co/sites/default/files/archivos_paginas/pr-tic-_05_v1_seguridad_digital.pdf*



| | | |
|---|---|---|
| ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE CULTURA, RECREACIÓN Y DEPORTE | **GESTION OPERATIVA DE TI** | CÓDIGO: GOT-MN-02 |
| | **MANUAL PARA LA IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN** | VERSIÓN: 01 |
| | | FECHA: 01-02-2022 |
| | | **PÁGINA:** 4 DE 22 |

**1. OBJETIVO**

Establecer la metodología que oriente a los funcionarios públicos y contratistas para la identificación, actualización, clasificación y valoración del inventario de Activos de Información de la Secretaría Distrital de Cultura, Recreación y Deporte en adelante identificada con la sigla SDCRD, cuya finalidad es la protección de la confidencialidad, integridad y disponibilidad de la información institucional.

*Ilustración 12. Captura de pantalla del documento denominado "Manual para la identificación y clasificación de activos de información (GOT-MN-02)"*

### 3.2.3.1. Inventario de activos de información en la SCRD

Durante el desarrollo de a la auditoría se evidenció que la Secretaría utiliza el "Manual para la Identificación de Activos de Información (GOT-MN-02) para el desarrollo de esta actividad. La oficina de Tecnologías de la Información (OTI) compartió el documento denominado "CONSOLIDADO MATRIZ INVENTARIO ACTIVOS DE INFORMACIÓN SCRD 2022VF.xlsx", el cual contiene un listado de 135 activos de información identificados a octubre de 2022.

Se evidenció que en la "Cultunet"[33] se encuentra publicado el registro de activos de información y el índice de información clasificada y reservada de la SCRD del año 2019. Durante el desarrollo de la auditoría no se evidenciaron las publicaciones[34] ni los documentos de los años 2020, 2021 y 2022:

33 *Ubicado en el menú "MIPG", título "Documentación transitoria de los procesos V.8", Procesos de apoyo, Gestión de TIC.*

34 *El decreto 1081 de 2015 que reglamenta la ley 1712 de 2014, indica en el numeral 2.1.1.2.1.4 "Los sujetos obligados… …deben publicar en la página principal de su sitio web oficial… … (2) El Registro de Activos de Información; (3) El índice de Información Clasificada y Reservada; (4) El Esquema de Publicación de Información."*

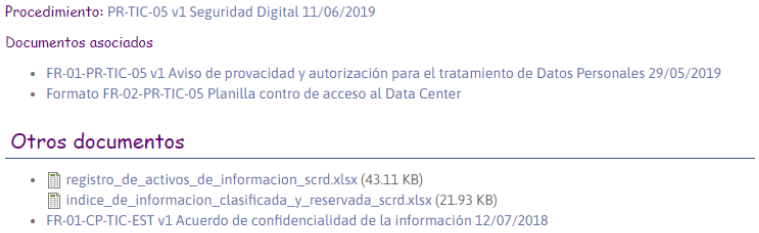



*Ilustración 13. Relación de documentos encontrados en la ubicación en "Cultunet" menú "MIPG", título "Documentación transitoria de los procesos V.8"  Procesos de apoyo  Gestión de TIC*


*Ilustración 14. Captura de pantalla del "Registro de activos de información" encontrado en la página web de la SCRD. Enlace: https://ant.culturarecreacionydeporte.gov.co/es/transparencia-y-acceso-a-la-informacion-publica/7-1-1-registros-de-activos-de-informacion*

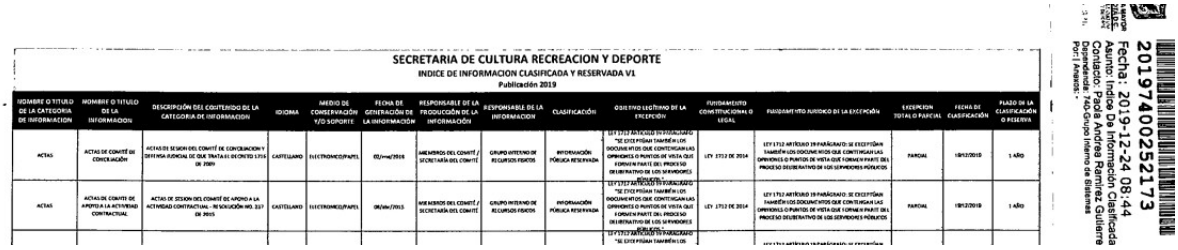



*Ilustración 15. Captura de pantalla del documento publicado en la pagina web de la Secretaría. Enlace: https://ant.culturarecreacionydeporte.gov.co/sites/default/files/documentos_transparencia/indice_de_informacion_clasificada_y_reservada_2019_20197400252173.pdf*

Se evidenció que el proceso de actualización de inventarios de activos de información en la SCRD se encuentra en desarrollo y, de acuerdo con el "Plan de Seguridad de la Información (GOT-PN-02)", esta actividad finalizó el 30 de noviembre de 2022.

Sobre este hecho, se encontró que el levantamiento de activos de información en relación con el proceso de la dirección de "Lectura y Bibliotecas" no se ha desarrollado. En la matriz de activos compartida durante el desarrollo de la auditoría se evidenciaron seis (6) activos de información[35] asociados a esta dirección, sin embargo, durante la entrevista de auditoría se evidenció que esta actividad no se ha desarrollado, pese a que la dirección

35 *Los seis (6) activos de información tienen el mismo nombre "RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED"*

de “Lectura y Bibliotecas” la conforman aproximadamente 40 empleados de planta y contratistas y unos 500 colaboradores contratados a través de dos operadores.

Así mismo, dicha dirección manifestó contar con su propio registro de activos de información y matrices de riesgos asociadas.

| IDENTIFICACIÓN GENERAL DEL ACTIVO | | | | TIPO DE ACTIVO | PROPIEDAD | | |
|---|---|---|---|---|---|---|---|
| | Dependencia | Nombre del activo | Descripción del activo | Tipo | Propietario de la información | Custodio | |
| ON ES AS ES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED | REGISTRA Y GENERA REPORTES DE TODAS LAS | INFORMACIÓN | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | A |
| ON ES AS ES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED | REGISTRA LA INFORMACIÓN DE LA MISIONALIDAD | INFORMACIÓN | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | A |
| ON ES AS ES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED | INFRAESTRUCTURA TECNOLÓGICA DE | HARDWARE | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE | D |
| ON ES AS ES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED | SOFTWARE UTILIZADO POR BIBLORED | SOFTWARE | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE | D |
| ON ES AS ES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED | PORTALES Y MICROSITIOS DE LA RED DISTRITAL DE | INFORMACIÓN | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE | D |
| ON ES AS ES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | BASES DE DATOS PERSONALES DE LA RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE BOGOTÁ - BIBLORED | BASES DE DATOS PERSONALES DE LA RED | BASES DE DATOS PERSONALES | DIRECCIÓN DE LECTURA Y BIBLIOTECAS | RED DISTRITAL DE BIBLIOTECAS PÚBLICAS DE | D |

*Ilustración 16. Captura de pantalla de los activos de información relacionados con la Dirección de Lectura y Bibliotecas*

### 3.2.3.2. Valoración de los riesgos de seguridad de la información

La evaluación de riesgos es el núcleo del SGSI[36] que se implementará en la SCRD. Será una metodología adecuada la que permita minimizar los potenciales riesgos de integridad, confidencialidad y disponibilidad del inventario de activos de información de la Secretaría. Durante el desarrollo de la auditoría se evidenció que la SCRD cuenta con una Política de Administración del Riesgo (DES-POL-01), un Proceso de Gestión de Riesgos (DES-PR-09[37]) publicado el 30 de agosto de 2022 y un manual de Gestión de Riesgos de Seguridad de la Información (DES-MN-04[38]) publicado el 8 de septiembre de 2022, el cual se encontró alineado con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5 del Departamento Administrativo de la Función Pública.

Se evidenció que la gestión de riesgos de Seguridad y Privacidad de la Información que se adelanta en la SCRD se encuentra en desarrollo. De acuerdo con el “Plan de Seguridad de la Información (GOT-PN-02)”, esta actividad finalizará el 30 de junio de 2023 y dependerá de la identificación y clasificación de los activos de información en la

36 *SGSI o Sistema de Gestión de Seguridad de la Información*.

37 *https://intranet.culturarecreacionydeporte.gov.co/sites/default/files/archivos_paginas/ultima_version_pr_gestion_de_riesgos_1.pdf*

38 *https://intranet.culturarecreacionydeporte.gov.co/sites/default/files/archivos_paginas/manual_de_gestion_de_riesgos_de_seguridad_de_la_informacion_v1_0.pdf*

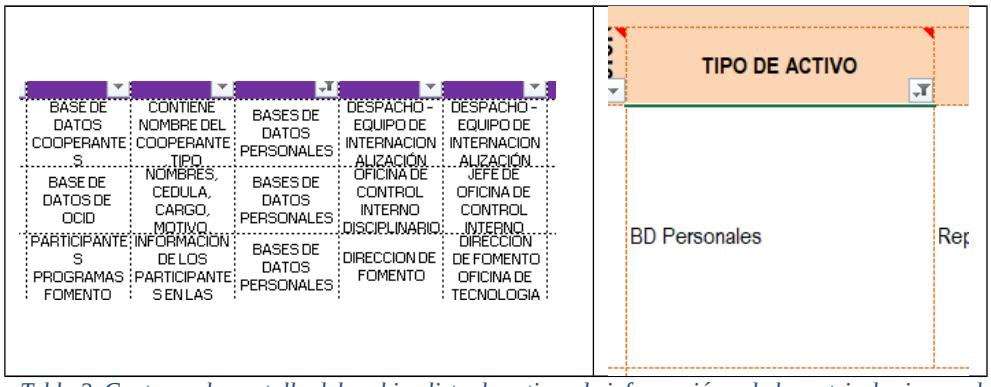
Secretaría, que como se mencionó en el ítem “Inventario de activos de la SCRD”, no ha concluido.

Durante el desarrollo de la auditoría, la Oficina de Tecnologías e Información (OTI) compartió seis (6) matrices de riesgo, aprobadas y relacionadas con los procesos de “Despacho”, “Dirección de Economía, Estudios y Política”, “Dirección de Gestión Corporativa”, “Grupo Interno de Trabajo de Gestión Financiera”, “Grupo Interno de Trabajo de Gestión de Talento Humano” y “Grupo Interno de Trabajo de Contratación”, sobre las mismas se indica lo siguiente:

- Cinco de las seis matrices se encuentran aprobadas.

- La valoración de los riesgos de seguridad de la información es una actividad dinámica, es decir, los resultados de la monitorización y medición de los controles propuestos pueden sugerir implementar nuevos controles o gestionar los riesgos con nuevos métodos o herramientas.

- Se sugiere mantener similitud en los nombres de los campos “tipo de activo” en la lista de activos de información y las matrices de riesgo. Se encontró que el tipo de activo denominado “Bases de datos personales” se escribe de manera diferente en el campo de las matrices de riesgo. Mantener la similitud en este campo evita posibles confusiones durante el análisis de riesgos para estos activos de información:



| | | | | |
|---|---|---|---|---|
| BASE DE DATOS COOPERANTES | CONTIENE NOMBRE DEL COOPERANTE TIPO | BASES DE DATOS PERSONALES | DESPACHO - EQUIPO DE INTERNACIONALIZACIÓN | DESPACHO - EQUIPO DE INTERNACIONALIZACIÓN |
| BASE DE DATOS DE OCID | NOMBRES, CEDULA, CARGO, MOTIVO | BASES DE DATOS PERSONALES | OFICINA DE CONTROL INTERNO DISCIPLINARIO | JEFE DE OFICINA DE CONTROL INTERNO |
| PARTICIPANTES PROGRAMAS FOMENTO | INFORMACION DE LOS PARTICIPANTES EN LAS | BASES DE DATOS PERSONALES | DIRECCION DE FOMENTO | DIRECCION DE FOMENTO OFICINA DE TECNOLOGIA |



*Tabla 2. Capturas de pantalla del archivo lista de activos de información y de la matriz de riesgos del proceso “Direccionamiento estratégico”*

- Se evidenció que la gestión de riesgos se realiza por proceso y por agrupación de activos de información como lo indica el Manual (DES-MN-04) y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5 del DAFP.

- Se evidenció que en algunas matrices la evaluación de los riesgos de seguridad de la información se encuentra incompleta, es decir, en unas se analizaron los riesgos de confidencialidad, en otras, se analizaron los de integridad y en otras, los de disponibilidad. Sin embargo, de acuerdo con la política de Administración de Riesgos (DES-POL-01) y el Manual de Gestión de Riesgos de la SCRD, se deberán analizar los riesgos por activo o grupos de activos y en las tres categorías, por pérdida de “confidencialidad”, “integridad” y “disponibilidad”:

- Para riesgos de Seguridad de la información:
  - Identificar los activos de Información.
  - Se identificará el riesgo a partir de la Pérdida de la confidencialidad, integridad y disponibilidad.
  - Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

*Ilustración 17. Captura de pantalla del numeral “2. Identificación del Riesgo” de la política de Administración de Riesgos de la SCRD.*

- No se evidenciaron implementados mecanismos de medición para cada uno de los controles propuestos en las matrices revisadas. Estos mecanismos o indicadores permitirían identificar si los controles propuestos son suficientes y eficaces, lo que ayudaría a evidenciar si la “zona de riesgo final” podrá mantenerse en el nivel actual o aumentar; esto último llevaría a la implementación de nuevos controles que ayudarían a prevenir las posibles amenazas y a prevenir la materialización de riesgos de seguridad de la información.

- Se sugiere agregar en el apartado “12.3 Evaluación del riesgo” del Manual de Gestión de Riesgos (DES-MN-04) de la Secretaría, como mecanismo de control adicional, los encontrados en el anexo A de la ISO 27001:2013, como lo sugiere la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5:

**5.4 Controles asociados a la seguridad de la información**

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

*Ilustración 18. Captura de pantalla del apartado “5.4 controles asociados a la seguridad de la información” de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5*

- Se evidenció la evaluación y análisis de riesgos de Seguridad de la información de 51 de los 135 activos de información listados en la matriz "CONSOLIDADO MATRIZ INVENTARIO ACTIVOS DE INFORMACIÓN SCRD 2022VF.xlsx", compartida por la OTI durante el desarrollo de la auditoría. Se sugiere continuar con el análisis y evaluación de los riesgos de los restantes 84 activos de información, a fin de valorar el impacto y la probabilidad de potenciales amenazas a la integridad, confidencialidad y disponibilidad; esto para proponer controles con el propósito de mitigar los riesgos de Seguridad y de la Información de estos activos de información en la SCRD.

### 3.2.3.3. Plan de tratamiento de los riesgos de seguridad de la información y declaración de aplicabilidad

Durante el desarrollo de la auditoría no se evidenció un procedimiento para desarrollar el "tratamiento de los riesgos de seguridad de la información" en la SCRD, en el cual se debería registrar la selección de controles, de acuerdo con los riesgos identificados en la evaluación hecha para cada proceso. El resultado de esta actividad sería un documento donde se evidenciaría la selección de controles para cada riesgo identificado, así como la aceptación del dueño del proceso para implementarlos en la siguiente fase.

El "Plan de tratamiento de riesgos" será un documento aprobado por la dirección en el cual se planificarán las actividades que se desarrollarán en la fase de implementación del MSPI. Este documento se encontró en la Secretaría descrito como "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (GOT-PN-03)[39]"

Durante el desarrollo de la auditoría se evidenció el documento denominado "Declaración de Aplicabilidad Anexo A ISO 27001:2013" de la SCRD, publicada en el año 2017, en la cual se expresa que la SCRD tendrá *"…en cuenta los 114 controles agrupados en 35 objetivos de control y 14 dominios en la última versión de esta norma, de los cuales la Secretaría Distrital de Cultura, Recreación y Deporte aplicará los 114 controles del Anexo A para la implementación del SGSI..."*

Así mismo, se evidenció que la revisión de este documento se debería haber hecho anualmente, sin embargo, durante el desarrollo de la auditoría no se encontraron las versiones actualizadas del documento "Declaración de Aplicabilidad" correspondientes a los años 2018, 2019, 2020, 2021 y 2022:

39 Este documento se tratará en la fase de "operación y/o implementación"

Durante la revisión y evaluación de implementación de buenas prácticas, se tienen en cuenta los 114 controles agrupados en 35 objetivos de control y 14 dominios en la última versión de esta norma, de los cuales la **Secretaría Distrital de Cultura, Recreación y Deporte** aplicará los 114 controles del **Anexo A** para la implementación del SGSI.

La revisión y evaluación de esta Declaración de Aplicabilidad se realizará de manera anual y los resultados serán presentados en la Revisión por la Dirección y en el Sistema Integrado de Gestión.

*Ilustración 19. Captura de pantalla del documento denominado "Declaración de Aplicabilidad Anexo A ISO 27001:2013" de la SCRD, publicado en el año 2017*

### 3.2.3.4. Competencia, toma de conciencia y comunicación

La SCRD cuenta con un "Plan de capacitación, sensibilización y comunicación de seguridad de la información (GOT-PN-01)", publicado el 28 de junio de 2022. Se evidenció que el plan de capacitación y sensibilización de seguridad de la información aún no ha llegado a la totalidad de la población de la SCRD, sin embargo, se evidenció el cumplimiento de lo indicado en el numeral "12.6 Seguimiento a indicadores", la cobertura de sensibilización se haría a unos 80 funcionarios / contratistas. Sobre el particular, la Oficina de Tecnología e Información (OTI) compartió actas de asistencia a algunos eventos de Seguridad de la Información realizados en la Secretaría donde se evidencia que este indicador cumplió, en relación con los siguientes temas:

- 9-23 Lineamientos Operativos TI
- 9-7 Charla de seguridad
- 6-24 Gestión Incidentes CSIRT
- 3-18 RBND por Sonia
- 2-24 Seguridad ComparTIC
- 2-22 Acuerdo Marco ACTIC
- 2-22 Activos de Información

En los documentos compartidos por la OTI no se evidenció la sensibilización en los siguientes temas que se indicó, así se haría:

- Taller de Hacking ético e Ingeniería Social
- Analítica
- Servicios seguros en continuidad del negocio
- Clasificación, análisis y riesgos de los datos
- Planeación estratégica de Tecnologías de la Información y las Comunicaciones
- Taller de buenas prácticas en seguridad de sitios Web
- Desarrollo de Software

## 3.3. Fase 3: Operación y/o implementación

Durante el desarrollo de la auditoría se evidenció un avance del 4% en esta fase:

| COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
|---|---|---|
| Planificación | 20% | 40% |
| **Implementación** | **4%** | **20%** |
| Evaluación de desempeño | 3% | 20% |

*Ilustración 20. Se observa porcentaje de avance encontrado en la SCRD en relación con la fase de "implementación" del MSPI*

La fase de operación[40] y/o implementación del Modelo de Seguridad y Privacidad de la Información – MSPI tiene por objeto el "hacer" en el ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Durante esta fase, se llevará a cabo la implementación de los "controles" para dar cumplimiento al MSPI:


*Ilustración 21. Diseño de la fase de operación o "implementación" sugerida en el MSPI propuesto por el MINTIC.*

En los siguientes títulos se explicará con mayor detalle los hallazgos identificados:

40 Esta fase se encuentra descrita en la cláusula No. 8 y en el anexo A del estándar ISO 27001:2013.

### 3.3.1. Planificación e implementación

El Modelo de Seguridad y Privacidad de la Información – MSPI exige que en esta fase se desarrollen dos documentos:

- Un plan de implementación de controles de seguridad y privacidad de la Información, el cual deberá estar aprobado por la dirección.
- Documento donde se evidencie la implementación de cada control de Seguridad y Privacidad de la Información.

Durante el desarrollo de la auditoría no se evidenciaron elaborados estos documentos. La puesta en marcha del MSPI en la SCRD deberá hacerse en la siguiente vigencia. Sin embargo, el desarrollo de la fase de operación requiere finalizar las actividades de la fase anterior, esto es, atender y priorizar los siguientes aspectos para llevar a feliz término la implementación del MSPI en la SCRD:

- La SCRD deberá formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en la SCRD, trasversal a la entidad y cercano a la dirección.

- Se deberá formalizar la asignación de recursos para la implementación del MSPI en la SCRD. El modelo propuesto por el MINTIC, alienado con la norma ISO 27001:2013, deberá contar con recursos para lograr los objetivos propuestos a mediano y largo plazo y que se describan en el *"plan de implementación de controles de seguridad y privacidad de la Información"*.

- Se deberá finalizar con el levantamiento de activos de información en la SCRD, para luego concluir la evaluación y valoración de los riesgos de Seguridad y Privacidad de la Información de la totalidad de activos de información identificados. Estas actividades serán la base para la implementación de los controles que ayudarán a mitigar los riesgos en la fase No. 3 de operación y/o implementación donde serán desarrollados. La gestión de riesgos deberá ser dinámica y sistemática en cada uno de los procesos de la SCRD.

- Se deberán formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI de la SCRD. 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 los que se describan los lineamientos para gestionar la Seguridad de la Información en la SCRD.

### 3.3.2. Controles de seguridad de la información

Un control es el conjunto de actividades que se desarrollarán tendientes a mantener los riesgos por debajo del "nivel de riesgo asumido". El uso de controles se deberá desarrollar en la fase de "Planificación", para luego implementar en la fase de "Operación y/o Implementación" del MSPI.

La lista de los controles propuestos en el MSPI se encuentra relacionada en el numeral "6. Tabla de controles" del documento denominado "Controles de Seguridad y Privacidad de la Información"[41] propuesto por el MINTIC, la cual se encuentra alineada con los definidos en el anexo A de la ISO/EIC 27001:2013.

Los controles de la lista del anexo A podrán utilizarse en dos momentos: i) como parte del proceso de mitigación de los riesgos de seguridad de la información; ii) como mecanismos de control cuando exista un plan de acción o de tratamiento de riesgos de seguridad de la información, es decir, cuando se evidencie la posible materialización de un riesgo de seguridad.

Durante el desarrollo de la auditoría se hizo la evaluación de cada uno de los 113 controles encontrados en el Anexo A de la ISO/EIC 27001 propuestos por el MINTIC, con el objetivo de evidenciar si estos han sido utilizados como parte de la "mitigación" o de "tratamiento" de los riesgos de seguridad.

Se usó la siguiente nomenclatura que ayudará a entender el estado de cada uno, así mismo, se anexará este documento como parte del informe auditor (Ver **Anexo No. 01**)

| Estado | Descripción |
|---|---|
| Cumple satisfactoriamente | El control existe, se encontró gestionado, se está cumpliendo con lo que la norma solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI de la SCRD. |
| Cumple parcialmente | Lo que la norma solicita se está haciendo de manera parcial, se está haciendo diferente, no está documentado, pero se desarrollan actividades, se definió, pero no se gestiona. |
| No cumple | No existe, se evidenció que no se están desarrollando actividades, |
| No aplica | El control no es aplicable para la entidad. |

41 https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150511_G8_Controles_Seguridad.pdf

El resultado de la evaluación hecha a los 113 controles encontrados en el Anexo A se resume[42] en la siguiente imagen:


*Ilustración 22. Gráfico con los porcentajes de avance de "implementación" de los 113 controles del Anexo A de la ISO/EIC 27001.*

- El 11% de los controles se encontraron gestionados, es decir, se evidenció que se encuentran documentados y gestionados.

- El 79% de los controles se encontró en un "cumplimiento parcial". Sobre estos, se evidenciaron diferentes causas que se resumirán de la siguiente manera:

    - Se encontró documentada la política en relación con el control, sin embargo, no se encontraron documentados los procedimientos, manuales y guías con los lineamientos que se deberían hacer entorno a la política.
    - Se evidenciaron actividades desarrolladas por el equipo de seguridad de la SCRD, sin embargo, no se encontraron documentadas.

- El 9% de los controles no se encontraron desarrollados. En este ítem, se encuentra el relacionado con la gestión de incidentes de seguridad de la información en la SCRD. Durante el desarrollo de la auditoría se evidenció el reporte[43] de un incidente, que ocurrió entre el 5 y el 8 de agosto de 2022, como consecuencia de la materialización de riesgos de seguridad de la información de diferentes activos de la SCRD. Sin embargo, la resolución del incidente no siguió

42 En el anexo 1 del presente informe, se encontrarán desarrollados cada uno de los 113 controles y las sugerencias que se estimaron deberán desarrollarse.

43 Radicación de Orfeo No. 20221400309593 con descripción "Solicitud de Información Contingencia agosto 05 a 08 de 2022"

los lineamientos propuestos en la guía No. 21, “Gestión de Incidentes”[44] sugeridos por el MINTIC como parte del MSPI.

- El 1% de los controles se evidenció que puede no ser aplicables a la SCRD. Esto deberá ser parte del análisis de gestión de riesgos y será del resultado de éste el que indique si el control es o no aplicable para la SCRD.

### 3.3.3. Gestión de riesgos y el plan de tratamiento

En esta fase, la gestión de riesgos se hace a intervalos planificados, es decir, se deberá documentar las revisiones que se realicen a las matrices de riesgos de la Seguridad de la Información de la SCRD.

Durante el desarrollo de la auditoría se evidenció el documento denominado “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (GOT-PN-03)”, publicado el 31 de enero de 2022, en el que se evidenciaron las actividades que se desarrollarían en la fase de “implementación” del MSPI en la SCRD.

De acuerdo con el numeral “2. Identificación de Riesgo” relacionado con los “Niveles de aceptación del riesgo” de la Política de Administración de Riesgos (DES-POL-01) y el numeral “13. Tratamiento de los riesgos” del “Proceso de Gestión de Riesgos (DES-PR-09)” de la SCRD, este plan se activará si el resultado es igual o superior a “ALTO”. Sin embargo, la política y el manual también advierten que se deberá hacer seguimiento semestral de los controles propuestos y evidenciarlos en el “instrumento destinado” para tal fin, como se evidencia en la siguiente captura de pantalla:

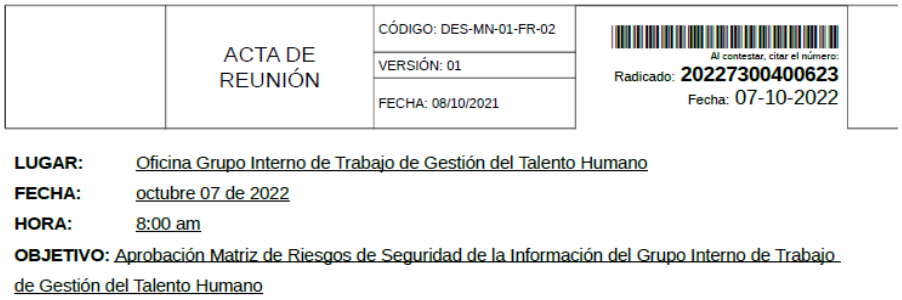
| Riesgo | Nivel de Aceptación | Zona de Riesgo Inherente | Gestión del Riesgo | Seguimiento Primera y Segunda línea de defensa (OAP) |
|---|---|---|---|---|
| SEGURIDAD DE LA INFORMACIÓN | | BAJA | Se deben mantener los controles existentes | Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el instrumento destinado. |
| | **APETITO** | MODERADA | | |
| | **TOLERANCIA** | ALTA | Se deben establecer nuevos controles o fortalecer los existentes que permitan reducir el riesgo. | |
| | | EXTREMA | | |

*Ilustración 23. Captura de pantalla encontrada en dos documentos: i) En el numeral “2. Identificación de Riesgo” relacionada con los “Niveles de aceptación del riesgo” de la Política de Administración de Riesgos (DES-POL-01) y, ii) en el numeral “13. Tratamiento de los riesgos” del “Proceso de Gestión de Riesgos (DES-PR-09)” de la SCRD.*

La revisión de las seis (6) matrices de riesgo compartidas por la Oficina de Tecnologías de Información (OTI) dan cuenta que la valoración de los riesgos de seguridad de la información se encuentra en los niveles “BAJO” y “MODERADA”. A así mismo, se

44 https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

evidenció que cinco (5) de las seis (6) matrices compartidas por la OTI fueron aprobadas en octubre de 2022, por consiguiente, no se ha cumplido el primer semestre para el seguimiento a los controles existentes:



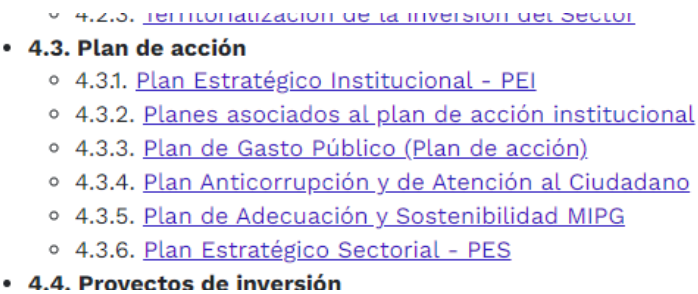
| | ACTA DE REUNIÓN | CÓDIGO: DES-MN-01-FR-02<br>VERSIÓN: 01<br>FECHA: 08/10/2021 | Al contestar, citar el número: Radicado: **20227300400623** Fecha: 07-10-2022 |
|---|---|---|---|

**LUGAR:** Oficina Grupo Interno de Trabajo de Gestión del Talento Humano
**FECHA:** octubre 07 de 2022
**HORA:** 8:00 am
**OBJETIVO:** Aprobación Matriz de Riesgos de Seguridad de la Información del Grupo Interno de Trabajo de Gestión del Talento Humano

*Ilustración 24. Captura de pantalla del acta de aprobación de la matriz de riesgos del Grupo Interno de Trabajo de Gestión de Talento Humano.*

Por otra parte, no se evidenció publicado en la página web de la Secretaría el “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”, así como 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. Integración de los planes institucionales y estratégicos al plan de acción”* del decreto 612 del 4 de abril de 2018, que indica que las entidades del Estado deberán *“integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año”*

La siguiente captura de pantalla corresponde al menú “Transparencia acceso información pública” donde se sugiere, debería ubicarse esta información:



- 4.2.3. Territorialización de la inversión del Sector
- **4.3. Plan de acción**
  - 4.3.1. Plan Estratégico Institucional - PEI
  - 4.3.2. Planes asociados al plan de acción institucional
  - 4.3.3. Plan de Gasto Público (Plan de acción)
  - 4.3.4. Plan Anticorrupción y de Atención al Ciudadano
  - 4.3.5. Plan de Adecuación y Sostenibilidad MIPG
  - 4.3.6. Plan Estratégico Sectorial - PES
- **4.4. Proyectos de inversión**

*Ilustración 25. Captura de pantalla página web de la Secretaría de Cultura, Recreación y Deporte (SCRD); enlace: https://www.culturarecreacionydeporte.gov.co/es/transparencia-acceso-informacion-publica*

No obstante, se evidenciaron publicados estos documentos en la “Cultunet” de la SCRD, como se muestra a continuación:

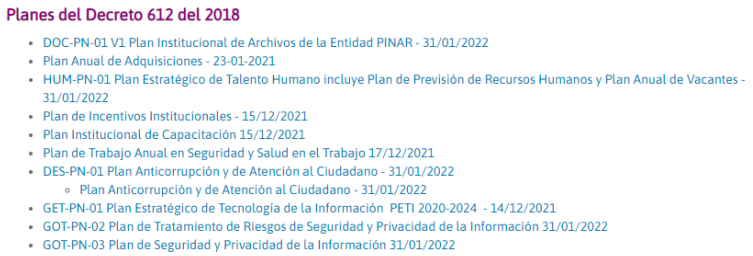



*Ilustración 26. https://intranet.culturarecreacionydeporte.gov.co/mipg/documentos-estrategicos*

Durante esta fase se deberán desarrollar los indicadores de Seguridad y Privacidad de la Información. Durante el desarrollo de la auditoría no se evidenciaron los indicadores para monitorizar el MSPI que se implementarán en la SCRD, como tampoco un procedimiento para el desarrollo de estas actividades.

## 3.4. Fase 4: Evaluación de desempeño

Esta fase tiene por objetivo la evaluación del desempeño y eficiencia del Modelo de Seguridad y Privacidad de la Información en la SCRD. Hace parte del "Verificar" en el ciclo PHVA (Planear-Hacer-Verificar- Actuar). Durante el desarrollo de la auditoría se evidenció un avance del 3% en esta fase:

| COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
|---|---|---|
| Planificación | 20% | 40% |
| Implementación | 4% | 20% |
| **Evaluación de desempeño** | **3%** | **20%** |

*Ilustración 27. Se observa porcentaje de avance encontrado en la SCRD en relación con la fase de "Evaluación de desempeño" del MSPI*

El siguiente es el esquema propuesto por el MINTIC para el desarrollo de esta fase:


*Ilustración 28. Captura de pantalla de la fase de evaluación y desempeño del MSPI propuesto por el MINTIC*

### 3.4.1. Monitoreo, medición, análisis y avaluación

Durante el desarrollo de la auditoría no se evidenciaron indicadores relacionados con la Seguridad y Privacidad de la Información. La revisión de la *"Herramienta de administración de la Mejora y Seguimiento de Acciones por Proceso 2021"* evidenció la existencia de un "incumplimiento" relacionado con la gestión de riesgos y activos de información de "seguridad digital" que ya se gestionó.

El MSPI propone el desarrollo de una guía, que puede contemplar los lineamientos encontrados en el documento denominado "Guía de Evaluación del Desempeño" u otro similar.

Esta herramienta se debería utilizar como mecanismo de monitoreo y seguimiento a las actividades desarrolladas en el MSPI que se implementará en la SCRD.

### 3.4.2. Auditorías internas

La evaluación del MSPI se debería hacer a través de auditorías internas, que se sugiere realizar a intervalos planificados. Durante el desarrollo de la auditoría se evidenció que esta fue la primera auditoría que se hace al MSPI en la SCRD. Por consiguiente, no se cuenta con indicadores de evaluación para ser contrastados o para medir el avance de las actividades desarrolladas respecto al modelo implementado en la SCRD.

De igual manera, el MSPI que se implemente en la Secretaría deberá ser revisado[45] y aprobado en el Comité Institucional de Gestión y Desempeño, cuando así se considere, de tal manera que la Dirección podrá evaluar el avance desde la óptica estratégica.

45 Las evaluaciones del MSPI deberían ser a intervalos planificados, una sola reunión será suficiente para el cumplimiento de esta actividad.

## 3.5. Fase 5: Mejoramiento continuo

Esta fase tiene por objetivo la consolidación de los resultados de la fase de "Evaluación de desempeño" en el documento denominado "Plan de Mejora Continua" relacionado con el Modelo de Seguridad y Privacidad de la Información en la SCRD. Esta fase hace parte del "Actuar" en el ciclo PHVA (Planear-Hacer-Verificar- Actuar) y se evidenció que se lleva un avance del 2% en esta fase:

| COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
|---|---|---|
| Planificación | 20% | 40% |
| Implementación | 4% | 20% |
| Evaluación de desempeño | 3% | 20% |
| **Mejora continua** | **2%** | **20%** |

*Ilustración 29. Se observa porcentaje de avance encontrado en la SCRD en relación con la fase de "Mejora continua" del MSPI*

En la siguiente imagen se observa el modelo de esta fase propuesto por el MINTIC:

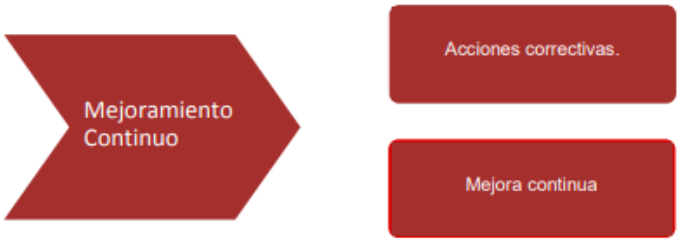



*Ilustración 30. Captura de pantalla de la fase de Mejoramiento Continuo del MSPI propuesto por el MINTIC*

El desarrollo del plan de mejora continua del MSPI en la SCRD deberá tener en cuenta dos tipos de resultados:

- Los resultados del plan de seguimiento, evaluación y análisis.
- Los resultados de ejecución de auditorías internas y revisiones independientes.

Sin embargo, no se encontraron indicadores, planes de acción o de mejora continua para hace evaluación o seguimiento al MSPI.

## 4. LIMITACIONES

No se presentaron limitaciones durante el ejercicio de la auditoría interna. Se reconoce la colaboración de los funcionarios de las unidades auditables, lo que facilitó la comprensión de la información presentada en procura de conocer el trabajo realizado en el marco del objetivo de la auditoría.

## 5. RESULTADOS DEL TRABAJO DE AUDITORÍA

Producto de la evaluación realizada, se presentan los siguientes resultados

| TIPO DE RESULTADO | CANTIDAD | REFERENCIACIÓN |
|---|---|---|
| Fortalezas | 0 | |
| Cumplimientos | 1 | 5.17 |
| Incumplimientos | 1 | 5.16 |
| Oportunidades de Mejora | 15 | 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, 5.12, 5.13, 5.14, 5.15. |
| **TOTAL:** | 17 | |

### 5.1. OPORTUNIDAD DE MEJORA: Actualizar el contexto

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.

### 5.2. OPORTUNIDAD DE MEJORA: Objetivos del SGSI

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[46]" propuesto por el MINTIC y lo descrito en la cláusula 1.0 del estándar ISO 27001:2013.

### 5.3. OPORTUNIDAD DE MEJORA: Formalizar el rol del responsable de la seguridad de la información

Se sugiere formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en la SCRD, trasversal 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[47]"

### 5.4. OPORTUNIDAD DE MEJORA: Formalizar la asignación de recursos para el desarrollo del MSPI

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)"

### 5.5. OPORTUNIDAD DE MEJORA: Activos de información

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

---

46 *https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf*

47 *El MINTIC propone la "Guía 4- Roles y responsabilidades" para desarrollar este ítem, sin embargo, la SCRD podrá incorporarla o no. Link: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150523_G4_Roles_responsabilidades.pdf*

Secretaría. Se encontró que esta actividad 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.

### 5.6. OPORTUNIDAD DE MEJORA: Gestión de riesgos

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 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 (DES-PR-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.

### 5.7. OPORTUNIDAD DE MEJORA: Tratamiento de los riesgos de seguridad de la información

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.

### 5.8. OPORTUNIDAD DE MEJORA: Formalizar procesos, guías e instructivos del MSPI

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.

Durante la revisión y evaluación hecha a los 113 controles encontrados en el ANEXO A de la ISO/EIC 27001, se evidenció que, el 79% de los controles se encuentran en un "cumplimiento parcial", es decir, se evidenciaron actividades, pero hay ausencia de documentación relacionada con procedimientos, manuales o guías que describan los lineamientos que se deberían ejecutar respecto a cada uno. Así mismo, el 9% de estos controles no se encontraron gestionados, es decir, no se evidenciaron actividades como tampoco documentación relacionada con los mismos.

El resultado de la evaluación realizada a los 113 controles encontrados en el Anexo A se resume[48] en la siguiente imagen:

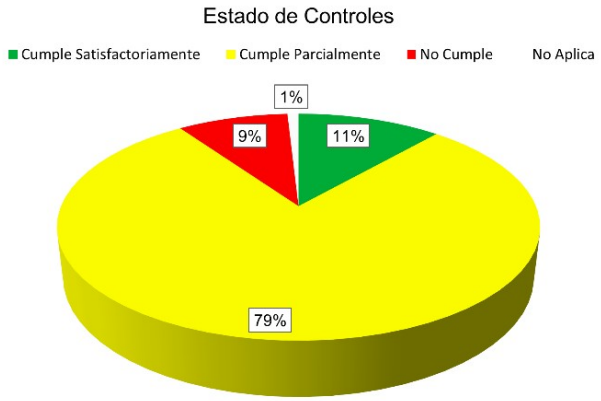



*Ilustración 31. Gráfico con los porcentajes de avance de "implementación" de los 113 controles del Anexo A de la ISO/EIC 27001.*

### 5.9. OPORTUNIDAD DE MEJORA: Actualizar "declaración de aplicabilidad"

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.

48 En el anexo 1 del presente informe, se encontrarán desarrollados cada uno de los 113 controles y las sugerencias que se estimaron deberán desarrollarse.

**5.10. OPORTUNIDAD DE MEJORA: Plan de capacitación, sensibilización y comunicación**

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.

**5.11. OPORTUNIDAD DE MEJORA: Documentos alojados en dos “menús” de Cultunet**

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”, 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)

**5.12. OPORTUNIDAD DE MEJORA: La OTI y el rol de seguridad de la Información como parte de la segunda línea de defensa de la SCRD**

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.

**5.13. OPORTUNIDAD DE MEJORA: Indicadores del MSPI**

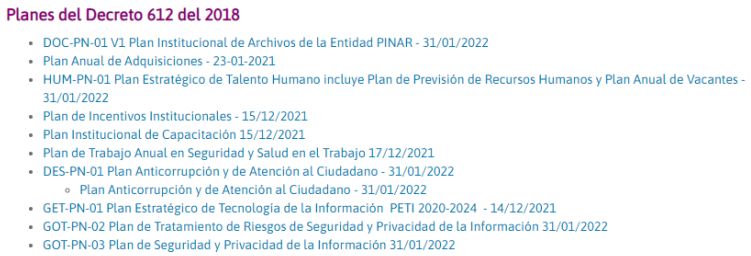
Se sugiere implementar un procedimiento para gestionar los indicadores y monitorizar las actividades de la implementación de Modelo de Seguridad y Privacidad de la Información en la Secretaría, de acuerdo con los dispuesto en la fase 4 “Evaluación y desempeño”, con el objetivo de medir el desempeño y eficiencia del sistema.

### 5.14. 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.

### 5.15. 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. Sin embargo, se evidenció que esta publicación se encuentra en la “intranet” o Cultunet de la Secretaría, tal como se evidencia a continuación:


Planes del Decreto 612 del 2018

- DOC-PN-01 V1 Plan Institucional de Archivos de la Entidad PINAR - 31/01/2022
- Plan Anual de Adquisiciones - 23-01-2021
- HUM-PN-01 Plan Estratégico de Talento Humano incluye Plan de Previsión de Recursos Humanos y Plan Anual de Vacantes - 31/01/2022
- Plan de Incentivos Institucionales - 15/12/2021
- Plan Institucional de Capacitación 15/12/2021
- Plan de Trabajo Anual en Seguridad y Salud en el Trabajo 17/12/2021
- DES-PN-01 Plan Anticorrupción y de Atención al Ciudadano - 31/01/2022
  - Plan Anticorrupción y de Atención al Ciudadano - 31/01/2022
- GET-PN-01 Plan Estratégico de Tecnología de la Información PETI 2020-2024 - 14/12/2021
- GOT-PN-02 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 31/01/2022
- GOT-PN-03 Plan de Seguridad y Privacidad de la Información 31/01/2022

*Ilustración 32. https://intranet.culturarecreacionydeporte.gov.co/mipg/documentos-estrategicos*

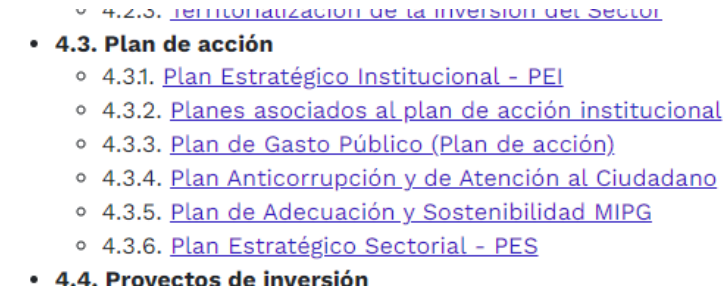

- 4.2.3. Territorialización de la inversión del Sector
- **4.3. Plan de acción**
  - 4.3.1. Plan Estratégico Institucional - PEI
  - 4.3.2. Planes asociados al plan de acción institucional
  - 4.3.3. Plan de Gasto Público (Plan de acción)
  - 4.3.4. Plan Anticorrupción y de Atención al Ciudadano
  - 4.3.5. Plan de Adecuación y Sostenibilidad MIPG
  - 4.3.6. Plan Estratégico Sectorial - PES
- **4.4. Proyectos de inversión**

*Ilustración 33. Captura de pantalla página web de la Secretaría de Cultura, Recreación y Deporte (SCRD); enlace: https://www.culturarecreacionydeporte.gov.co/es/transparencia-acceso-informacion-publica*

Se recomienda revisar y realizar las publicaciones donde corresponde.

### 5.16. 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.

### 5.17. CUMPLIMIENTO: Política de seguridad de la información y el plan de seguridad de la información

Se evidenció en la SCRD una política y un manual de políticas de Seguridad de la Información, los cuales se encuentran aprobadas por la dirección.

## 6. CONCLUSIONES

El Modelo de Seguridad y Privacidad de la Información en la Secretaría se encontró en un avance del 30%, resumido en cuatro (4) fases; planificación, implementación, evaluación de desempeño y mejora continua, 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% |

*Ilustración 3. Captura de pantalla del porcentaje de avance evidenciado durante el desarrollo de la auditoría.*

Se considera necesario el establecimiento de acciones correctivas y de mejora respecto de las desviaciones referidas en los incumplimientos y oportunidades de mejora resultado del trabajo de auditoría realizado.

## 7. RECOMENDACIONES

A modo de recomendación, se resaltan los siguientes aspectos:

7.1. Se sugiere priorizar y finalizar las actividades pendientes por desarrollar en la fase de “Planificación” para llevar a buen término la implementación y las demás etapas del Modelo de Seguridad y Privacidad de la Información en la SCRD.

7.1. Se sugiere formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en la SCRD, trasversal a la entidad y cercano a la dirección.

7.2. Se sugiere finalizar con el levantamiento de activos de información en la SCRD, para luego, concluir la evaluación y valoración de los riesgos de Seguridad y Privacidad de la Información de la totalidad de activos de información identificados. Estas actividades serán la base para la implementación de los controles que ayudarán a mitigar los riesgos en la fase No. 3 de operación y/o implementación donde serán desarrollados. La gestión de riesgos deberá ser dinámica y sistemática en cada uno de los procesos de la SCRD.

7.3. Se sugiere formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI de la SCRD. 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 los que se describan los lineamientos que se deberán hacer para gestionar la Seguridad de la Información en la SCRD.

7.4. 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 los dispuesto en la fase 4 “Evaluación y desempeño”, con el objetivo de medir el desempeño y eficiencia.

7.5. 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.

7.6. Actualizar y publicar 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” de la vigencia 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. Se sugiere contar con un indicador para monitorizar esta actividad que se deberá desarrollar anualmente.

## 8. PLAN DE MEJORAMIENTO

De acuerdo con lo indicado en el procedimiento para la mejora vigente en la Secretaría, 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.

## 9. FIRMAS

| Elaboró | Aprobó |
|---|---|
| **Marco Ramiro Marin Buitrago** | **Omar Urrea Romero** |
| **Contratista** | **Jefe Oficina Control Interno** |

**Nota:** La comunicación interna remisoria del presente informe se constituirá como el informe ejecutivo y debe incluir como mínimo el resumen del resultado.

**Documento 20221400541923 firmado electrónicamente por:**

**Omar Urrea Romero**, Jefe Oficina de Control Interno, Oficina de Control Interno, Fecha firma: 27-12-2022 08:45:42

062cde08d7561dcdb2cc9e73209c31d04711157e9c824bf44d410108abcfb41f