Bogotá D.C, jueves 28 de septiembre de 2023

PARA: CARLOS MAURICIO GALEANO VARGAS
Director general

DE: MARÍA DEL PILAR DUARTE FONTECHA
Asesora de Control Interno

ASUNTO: REMISIÓN INFORME FINAL AUDITORÍA INTERNA DE GESTIÓN MSPI DE IDARTES

Respetado Director.

De manera atenta anexo a esta comunicación el informe final de la auditoría interna al Modelo de Seguridad y Privacidad de la Información – MSPI del Idartes, cuyo objetivo correspondió a "*Determinar el estado actual de la gestión de seguridad información y privacidad de la información de Idartes mediante la auditoría interna, teniendo como referente el modelo MSPI y la norma NTC ISO/IEC 27001:2013.*

A continuación, se presentan los resultados de la auditoría, sobre los cuales se requiere la formulación de plan de mejoramiento y las recomendaciones.

Tipo de Resultado	Cantidad	Referenciación
Fortalezas	2	FO01, FO02
Cumplimientos	4	CU01, CU02, CU03 y CU04
Incumplimientos	1	IN01
Oportunidades de Mejora	8	OM01, OM02, OM03, OM04, OM05, OM06, OM07 y OM08
Total	**15**	

IN01. Tratamiento de los riesgos en seguridad de la información

El MSPI no está generando la Declaración de Aplicabilidad – SOA, la cual contiene los controles necesarios para implementar las opciones escogidas de tratamiento de riesgos en seguridad de la información y una justificación para la exclusión de controles del Anexo A. Documento firmado por alta dirección. (Requerimiento 6.1.3 d)

OPORTUNIDADES DE MEJORA

OM01. Planificación

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 pretende fortalecer la implementación en Idartes, de tal manera que se integren los procesos misionales, estratégicos y transversales, de acuerdo con lo propuesto en el numeral "8.2 Fase de planificación" del documento denominado "Modelo de Seguridad y Privacidad de la Información[1]" propuesto por el MINTIC y lo descrito en la cláusula 1.0 del estándar ISO 27001:2013.

OM02. Plan de capacitación, sensibilización y comunicación

Desarrollar e integrar un esquema de conocimiento y capacidades institucional para la cultura de la gestión de seguridad y privacidad de la Información con la participación activa de la Alta Dirección para la vigencia 2023, en el cual se debería involucrar de manera activa al Área de Comunicaciones y la Gestión de Talento Humano, para efectos de evidenciar la participación de la totalidad de funcionarios / contratistas de Idartes.

OM03. Integrar el MSPI al Sistema Integrado de Gestión – SIG y el Modelo Integrado de Planeación y Gestión - MIPG

A través del Decreto 591 de 2018 Idartes realizó la modificación del Sistema Integrado de Gestión Distrital (SIG) bajo los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG-, fortaleciendo los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto, sin embargo, hay una oportunidad de mejora para integrar la estrategia de la seguridad y privacidad de la información institucional del MSPI y re potencializar la gestión integral del talento humano, agilizar las operaciones, fomentar el desarrollo de una cultura organizacional sólida, promover la participación y confianza de la ciudadanía.

OM04. 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 el Instituto Distrital de Artes, trasversal a la entidad y dependiendo de 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[2]".

---

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

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

OM05. 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 el Idartes, de acuerdo con los dispuesto en la fase 4 “Evaluación y desempeño”, con el objetivo de medir el desempeño y eficiencia de los requerimientos y controles de MSPI.

OM06. Auditorías internas de gestión

Se sugiere incluir en el Plan Anual de Auditoría (PAA) la evaluación anual del Modelo de Seguridad y Privacidad de la Información – MSPI que se pretende implementar/operar en el Idartes, esto con el objetivo de dar cumplimiento a lo dispuesto en la fase 4 “Evaluación y desempeño” del MSPI.

OM07. Formalizar procesos, guías e instructivos del MSPI

Se sugiere formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI del Instituto. Como se evidenció, existe un conjunto de políticas descritas en el documento “Políticas de Seguridad y Privacidad de la Información del Idartes”, 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 y Privacidad de la Información del Instituto.

OM08. Actualización permanente del Instrumento MSPI

Se sugiere mantener actualizado el Instrumento MSPI como la herramienta de diagnóstico del Instituto en materia de seguridad y privacidad de la información que permita obtener un resultado preciso y oportuno en la construcción y mejora de los procesos de transformación digital necesarios y requeridos para atender los cambios culturales estratégicos, tácticos y operativos de la entidad, así como para el desarrollo de nuevas capacidades frente a las vulnerabilidades del entorno digital que puedan afectar los activos de información del Idartes en su principios de confidencialidad, disponibilidad e integridad.

Recomendaciones:

1. Fortalecer e incrementar la madurez del Modelo de Seguridad y Privacidad de la Información MSPI, ampliando el alcance del MSPI a todos los procesos del Instituto Distrital de las Artes – Idartes.

2. Mejorar la gobernanza y formalización de la gestión de Seguridad de la Información, Protección de Datos Personales y la Ciberseguridad. Se sugiere formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en el Instituto, trasversal a la entidad y dependiendo de la Dirección General.

3. Desarrollar e integrar un esquema de conocimiento y capacidades institucional para la cultura de la gestión de seguridad y privacidad de la Información con la participación activa de la Alta Dirección para la vigencia 2023, en el cual se debería involucrar de manera activa al Área de Comunicaciones y la Gestión de Talento Humano, para efectos de evidenciar la participación de la totalidad de funcionarios / contratistas de Idartes.

4. Incluir en el Plan Anual de Auditoría (PAA) la evaluación periódica del Modelo de Seguridad y Privacidad de la Información – MSPI que se pretende implementar en el Instituto Distrital de las Artes, esto con el objetivo de dar cumplimiento a lo dispuesto en la fase 4 “Evaluación y desempeño” del MSPI.

5. Integrar la estrategia de la seguridad y privacidad de la información - MSPI al Sistema Integrado de Gestión Distrital (SIG) y el Modelo Integrado de Planeación y Gestión - MIPG para fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto, re potencializar la gestión integral del talento humano, agilizar las operaciones, fomentar el desarrollo de una cultura organizacional sólida, promover la participación y confianza de la ciudadanía.

6. Probar este año el plan de continuidad TI que fortalezca la planificación, implementación, evaluación y mejora del MSPI, garantizando la restauración oportuna de las operaciones esenciales. Así mismo, como la correcta implementación de la gestión de la continuidad del servicio de TI, que disminuya la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, Idartes estaría preparada para responder en forma adecuada y oportuna de un daño potencial que pueda ser ocasionado por un incidente.

Con el estado actual del Modelo de Seguridad y Privacidad de la Información – MSPI 2023 del Idartes y con el plan de mejoramiento se convierte en un reto para el Instituto ser un referente del Sector Cultura, Recreación y Deporte del Distrito en la gestión de seguridad y privacidad de la información, por el resultado del nivel de madurez de las Instituciones que conforman.

Adicionalmente, se socializó la propuesta metodológica para la formulación del plan de mejoramiento resultante de la auditoría interna de gestión al Modelo de Seguridad y Privacidad de la Información MSPI con referentes de MIPG de la entidad y bajo la coordinación de la OAPTI, se realizará la formulación del plan de mejoramiento en el aplicativo Pandora, para el próximo 12 de octubre de 2023.

conforman el sector.

Atentamente,

Documento 20231300492683 firmado electrónicamente por:

MARIA DEL PILAR DUARTE FONTECHA, Asesora de Control Interno, Área de Control Interno, Fecha firma: 28-09-2023 14:36:42
Anexos: 1 folios

6e277b4f0e8a6ea3806e8ed69cf5a3e207f77e9fc120a3ad89c2ef4e25c2a31d
Codigo de Verificación CV: f1208 Comprobar desde:

INFORME PRELIMINAR DE AUDITORÍA INTERNA AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

ÁREA DE CONTROL INTERNO

INSTITUTO DISTRITAL DE LAS ARTES

BOGOTÁ D.C.

SEPTIEMBRE DE 2023

CONTENIDO

INTRODUCCIÓN

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

La gestión de la seguridad y privacidad de la información surge por la necesidad de proteger y salvaguardar la información propia de todas las partes involucradas del Instituto, la cual es de vital importancia y valor para las Entidades de Gobierno. Por tal motivo dicho ejercicio pretende revisar el cumplimiento de los requisitos del sistema de gestión de seguridad de la información que el Instituto ha implementado de acuerdo con la norma estandarizada ISO/IEC 27001:2013. Así mismo, revisar el cumplimiento de los lineamientos y requisitos del Programa Integral de Gestión de Datos Personales (PIGDP) y el nivel de madurez en la gestión de Ciberseguridad.

El Área de Control Interno, en desarrollo del plan anual de auditoría de la vigencia 2023 del Instituto Distrital de las Artes y en ejercicio de las facultades legales otorgadas por la Ley 87 de 1993 y demás normas concordantes, realizó en el marco del rol de seguimiento y evaluación, la auditoría interna al ***Modelo de Seguridad y Privacidad de la Información*** - ***MSPI,*** evaluando los requerimientos y la efectividad de los controles establecidos en la entidad, así como de aquellas actividades y procedimientos transversales establecidos en la entidad, que participan en el logro de los resultados organizacionales. La actividad de auditoría realizada por el equipo de control interno, contribuye al logro de los objetivos estratégicos, mediante las recomendaciones realizadas como producto de las desviaciones identificadas en desarrollo de la auditoría.

Esta auditoría fue realizada con base en la información suministrada por los líderes de los procesos de Instituto Distrital de Artes y entrevistas a los responsables de los mismos. Es responsabilidad de cada líder de proceso el suministro y contenido de la información base del análisis del proceso de aseguramiento.

La responsabilidad del Área de Control Interno se circunscribe a producir un informe que incluye los resultados de la auditoría ejecutada; las pruebas, procedimientos y análisis de la auditoría practicadas.

1. OBJETIVO

Determinar el estado actual de la gestión del Modelo de Seguridad y Privacidad de la información – MSPI en los procesos de Instituto Distrital de las Artes mediante la auditoría interna, teniendo como referente la norma NTC ISO/IEC 27001, lo cual permitirá generar un informe final de auditoría con hallazgos y oportunidades de mejora para ser implementados en el corto y mediano plazo.

2. ALCANCE

El período a evaluar es el comprendido entre el 01 de enero de 2023 y el 30 de junio de 2023, donde se realizará la auditoría interna al Modelo de Seguridad y Privacidad de la Información para los diecinueve (19) procesos de IDARTES, según los requisitos de la norma NTC ISO/IEC 27001:2013 y los objetivos de control contemplados en la norma NTC ISO/IEC 27002. Período de ejecución de la auditoría interna: Del 28 de junio al 28 de septiembre de 2023.

Alineación con los Objetivos Estratégicos del Instituto:

Objetivo N°2 “Fortalecer y transformar la cultura institucional, el clima organizacional, el vínculo de servidoras/es públicos, contratistas con el IDARTES, su apropiación misional y el sentido de pertenencia, para atender las demandas de la ciudadanía, la motivación y el reconocimiento de las/os servidoras/es”.

Objetivo N°3 “Generar la disponibilidad de recursos humanos y de infraestructura tecnológica, de alta calidad y eficiencia para la efectiva y oportuna operación de la entidad y de la gestión del conocimiento”.

3. METODOLOGÍA

Conforme con el Anexo 1 del Modelo de Seguridad y Privacidad de la Información del MinTIC y la Guía de auditoría interna basada en riesgos para entidades públicas, versión 4 expedida por el Departamento Administrativo de la Función Pública - DAFP, se utilizaron los procedimientos y/o técnicas de auditoría de: consulta, observación, inspección, revisión de comprobantes y procedimientos analíticos, con base en el ciclo PHVA (Planear, Hacer, Verificar, Actuar) incluido en el Manual Operativo del Modelo Integrado de Planeación y Gestión -MIPG y el Modelo de Seguridad de la Información – MSPI.

A continuación, se muestra en la figura, las fases desarrolladas en la auditoría interna MSPI:

Ilustración 1. Fases de la Auditoría Interna MSPI

Planear

- Definir el objetivo, el alcance y los tiempos de ejecución de la auditoría interna.
- Elaborar el programa de auditoría interna MSPI.
- Preparar los papeles de trabajo, realizar una revisión documental y procedimental sobre los procesos auditados y las actividades a realizar en las auditorías de campo.
- Definir fecha de la reunión de apertura.

Hacer

- Llevar a cabo la reunión de apertura el día 17 de julio de 2023.
- Ejecutar la auditoría a través de los procedimientos o técnicas de auditoría.
- Recolectar y analizar la información obtenida para la verificación del cumplimiento, de acuerdo con los criterios definidos en la auditoría.
- Elaborar y comunicar en la reunión de cierre el resultado del informe preliminar de auditoría a los líderes y/o responsables de los procesos auditados.
- Llevar a cabo la reunión de cierre el día 18 de septiembre de 2023.
- Elaborar y comunicar el resultado del informe final de auditoría a los líderes y/o responsables de los procesos auditados y al representante legal de la entidad.

Verificar

- Analizar las evidencias e información adicional entregada por los responsables de los procesos auditados, en respuesta al informe preliminar y determinar si hay lugar a retirar las observaciones detectadas por el equipo de control interno designado.

Actuar

- Incorporar las acciones formuladas por los responsables de los procesos, en el plan de mejoramiento por procesos, dispuesto en el aplicativo Pandora, lo anterior en caso de requerirse.

4. CRITERIOS DE AUDITORÍA. Normatividad

- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Decreto 2573 de 2014. “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- Resolución 344 de 2018, se adopta el Modelo Integrado de Planeación y Gestión MIPG y se crea el Comité Institucional de Gestión y Desempeño.
- Manual de Gobierno Digital para la Implementación de la Política de Gobierno Digital, entidades del orden nacional; MSPI; Formato Política SGSI – MSPI para la Política de Gobierno Digital, versión 7 de 2019.
- Guía para la gestión por procesos en el marco del Modelo Integrado de Planeación y Gestión - MIPG, DAFP, versión 1, 2020.
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital. “Establece medidas para desarrollar la confianza digital a través de la mejora la seguridad digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital”.
- Documento Maestro del Modelo de Seguridad y Privacidad de la Información – Anexo 1, versión 4 del MinTIC, 2021.
- Resolución 500 de 2021 de MinTIC, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de MSPI como habilitador de la política de Gobierno Digital.
- Plan Estratégico Institucional 2020-2024.
- Plan Estratégico de Tecnologías de Información – PETI 2023.
- Plan de Seguridad y Privacidad de la Información 2023.
- Instrumento de evaluación MSPI 2022 - 4 trimestre, diciembre 2022.
- Política de Seguridad de la Información, versión 4 - 2021
- Plan de tratamiento de riesgos de seguridad y privacidad de la información 2023.
- Las demás normas pertinentes relacionadas con el objetivo de la auditoría.

5. RIESGOS DE AUDITORÍA

Este riesgo se puede configurar, por la entrega de información inoportuna, incompleta, confusa o inexacta, lo que puede derivar en la probabilidad de emitir un concepto errado por parte de la auditora designada.

6. DESARROLLO DE LA AUDITORÍA

6.1 FASE 1. Entendimiento de necesidades y planeación

El plan de las sesiones presenciales de auditoría interna de gestión MSPI, se realizó exitosamente con los líderes y sus equipos de trabajo por cada uno de los procesos estratégicos, misionales y transversales del Instituto, cumpliendo con el contenido de las agendas programadas y revisando la visibilidad del MSPI como habilitador de la gestión de seguridad y privacidad de los activos de información del proceso.

Tabla 1. Programación de las Sesiones de Auditoría Interna MSPI

Id	Proceso	Líder del Proceso	Fecha Auditoría
SA00	Reunión de Apertura	Comité Institucional	Julio 17 de 2023
SA01	Gestión de Comunicaciones	Paola Andrea Méndez	Julio 26 de 2023
SA02	Evaluación Independiente	María del Pilar Duarte	Agosto 02 de 2023
SA03	Control Disciplinario	Martha Patricia Rincón M.	Agosto 02 de 2023
SA04	Gestión Financiera	Liliana Morales Ortiz	Agosto 02 de 2023
SA05	Relacionamiento con el Ciudadano	Liliana Morales Ortiz	Agosto 04 de 2023
SA06	Gestión Documental	Liliana Morales Ortiz	Agosto 09 de 2023
SA07	Gestión Espacios Integrales	Hanna Paola Cuenca	Agosto 11 de 2023
SA08	Gestión Bienes Servicios y Planta	Liliana Morales Ortiz	Agosto 11 de 2023
SA09	Gestión Jurídica	Sandra Vélez Abello	Agosto 14 de 2023
SA10	Gestión de Circulación Prácticas A.	Maira Ximena Salamanca	Agosto 14 de 2023
SA11	Gestión de Talento Humano	Liliana Morales Ortiz	Agosto 16 de 2023
SA12	Gestión del Conocimiento	Daniel Sánchez Rojas	Agosto 16 de 2023
SA13	Gestión Territorial	Leyla Castillo Ballén	Agosto 16 de 2023
SA14	Gestión Direccionamiento Estratégico	Daniel Sánchez Rojas	Agosto 18 de 2023
SA15	Gestión Tecnologías de Información	Daniel Sánchez Rojas	Agosto 18 de 2023
SA16	Gestión Fomento Prácticas Artísticas	Maira Ximena Salamanca	Agosto 18 de 2023
SA17	Gestión de Mejora Continua	Daniel Sánchez Rojas	Agosto 23 de 2023
SA18	Gestión de Participación Ciudadana	Daniel Sánchez Rojas	Agosto 23 de 2023
SA19	Gestión de Formación de Prácticas A.	Leyla Castillo Ballén	Agosto 23 de 2023
SA20	Visita Centro de Cómputo	Daniel Sánchez Rojas	Agosto 25 de 2023
SA21	Gestión de Ciberseguridad	Daniel Sánchez Rojas	Sept. 08 de 2023
SA22	Programa Integral Protección Datos	Sandra Vélez Abello	Sept. 14 de 2023

En el expediente de la auditoría interna MSPI No. 202310001909000005 se tiene registrado en la plataforma de Orfeo las actas de reuniones de cada una de las sesiones de auditoría realizadas y los soportes correspondientes.

6.2 FASE 2. Auditoría de Gestión de Seguridad y Privacidad de la Información

El marco de referencia para esta auditoría interna de gestión es el Instrumento o habilitador MSPI propuesto por el MINTIC desde el 2015, el cual se encuentra alineado con estándares nacionales e internacionales, como la norma NTC ISO/IEC 27001:2013, el marco de ciberseguridad del NIST, la norma ISO/IEC 31000, con el Marco de Referencia de Arquitectura de TI, el Modelo Integrado de Planeación y Gestión - MIPG, la Guía de Administración de Riesgos y el Diseño de Controles en entidades públicas, la Ley 1581 de 2012 de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras.

El Plan de Seguridad de la Información es trazado teniendo en cuenta los requerimientos y necesidades de las partes interesadas del MSPI, dado que la mayoría de la información generada en las diferentes Subdirecciones requiere de controles efectivos, de procedimientos internos para que permita brindar las condiciones para custodiar sus datos, sistemas de información, plan de tratamientos de riesgos de seguridad y privacidad de la información y acción para el uso y salvaguarda de la información.

Por lo anterior para la Oficina Asesora de Planeación y Tecnologías de la Información es un reto y una necesidad planear e implementar el Modelo de Seguridad y Privacidad de la Información - MSPI en Idartes de manera gradual y transversal, en sus procesos, tomando como piloto el proceso de Gestión de Tecnologías de la Información y las Comunicaciones TIC, por ser este el que tiene en gran medida en su haber, la seguridad de la información del Instituto.

A continuación, se describen cada una de las etapas[1] propuestas por el MinTIC a través del documento[2] maestro del MSPI y lo evidenciado durante el desarrollo de la auditoría en el Instituto Distrital de las Artes – Idartes.

6.2.1 Etapa de Diagnóstico. Tiene como objetivo identificar el estado actual del MSPI en el IDARTES a través de un análisis GAP o de brechas, que deberá desarrollarse a través de la herramienta de autodiagnóstico propuesta por el MinTIC. Durante el desarrollo de la auditoría, el Idartes compartió el documento denominado “Instrumento Evaluación MSPI 2023 2Trimestre”, en el cual se evidencia el cumplimiento de esta actividad.

---

[1] *Será de obligatorio cumplimiento para los sujetos obligados en la ley 1712 de 2014*
[2] *Documento Maestro del Modelo de Seguridad y Privacidad de la Información, enlace: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf*

Ilustración 2. Idartes Instrumento MSPI 2 Trimestre 2023 - Ciclo PHVA

Año	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	21%	40%
	Implementación	8%	20%
	Evaluación de desempeño	7%	20%
	Mejora continua	6%	20%
TOTAL		42%	100%

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.

6.2.2 Etapa de Planificación. Durante el desarrollo de la auditoría se evidenció un 21% de avance en esta etapa.

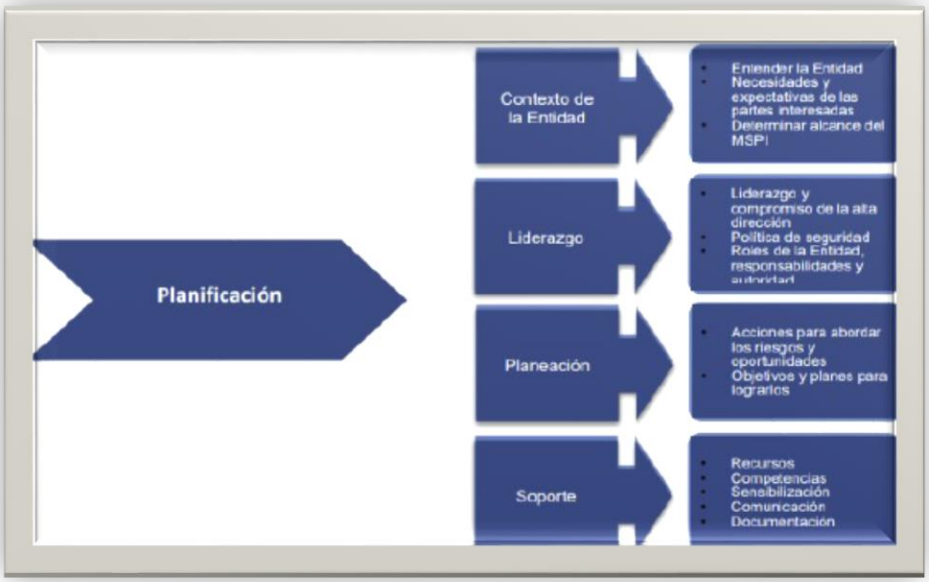
Ilustración 3. Idartes Instrumento MSPI 2 Trimestre 2023 - Etapa de Planificación

COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	21%	40%

Durante esta etapa, se deberán establecer las necesidades y los objetivos del MSPI, los cuales, deberán reflejar el alcance y los objetivos del Modelo de Seguridad y Privacidad de la Información - MSPI que se pretende implementar en el Idartes. Sobre el particular, durante el desarrollo de la auditoría, se evidenció el documento denominado "*Plan de Seguridad de la Información (GTI-P-02, v5*), publicado el 31 de enero de 2023, que algunas de estas actividades no han finalizado, se encuentran en desarrollo y tienen fechas de culminación para diciembre 31 de 2023.

El siguiente es el esquema propuesto por el MinTIC durante esta fase:

Ilustración 4. Captura de pantalla del MSPI de la etapa de planificación de MinTIC-2016



6.2.2.1 Contexto de la entidad

El contexto[3] de la entidad se encontró desarrollado en el apartado “Modelo Integrado de Planeación y Gestión - MIPG4” del Idartes, donde se evidenció una serie de documentos formalizados y relacionados con el contexto de la Institución. Se relacionan algunos documentos como muestra:

- Caracterización del Proceso de Direccionamiento Estratégico Institucional (DEI-C-01 v2).
- Procedimiento de la Implementación del Modelo Integrado de Planeación y Gestión – MIPG (DIR-PD-11 v1).
- Plan Estratégico Institucional 2020-2024 (DEI-PLEST-01 v2).
- Programa de Transparencia y Ética Pública – PTEP (DIR-PR-01 v1 2023).
- Portafolio de Servicios Artísticos y Culturales (DEI-PORT-01 v3)
- Protocolo para Publicación de Información de Conformidad con la Ley 1712 de 2014 (DEI-PROT-04 v1).
- Protocolo de Programación y Seguimiento a Proyectos de Infraestructura Cultural (1ES-DIR-PROT-02 v1).

[3] *El contexto de la organización se encuentra desarrollado en la cláusula número 4.0 de la norma ISO/IEC 27001:2013*
[4] *https://comunicarte.idartes.gov.co/SIG/direccionamiento-estrategico-institucional*

- Informe en cumplimiento a la Directiva 008 de 2021, con base en la gestión de la vigencia 2022.
- Plan Estratégico de Tecnologías de la Información – PETI (GTI-P-5).
- Políticas de Seguridad de la Información (GTI-POL-02 v4).
- Plan de Seguridad y Privacidad de la Información 2023 (GTI-P-02 v5).

En el documento denominado "Plan Estratégico de Tecnologías de la Información", se encontró que el PETI describe el estado actual, define la estrategia TI y los proyectos que ejecutará el Idartes durante los años 2020-2024, con actualizaciones anuales, para lograr los objetivos estratégicos alineados al Plan Estratégico Institucional y el marco de referencia de arquitectura empresarial del comprender, analizar, construir y presentar, con el enfoque de la estructuración del PETI alineado con los dominios definidos en el modelo de gestión Estrategia, Gobierno, Información, Sistemas de Información, Infraestructura de TI, Uso y Apropiación de TI y ***Seguridad de la información***.

Partes Interesadas de la Entidad

En el documento denominado "Plan Estratégico de Tecnologías de la Información - PETI", se encontró que uno de los motores estratégicos relacionados con el tema en IDARTES es "Garantizar la capacidad tecnológica que dé solución a las necesidades de las dependencias, áreas y partes interesadas".

Además, en el mismo documento sobre ***Calidad y Seguridad de los componentes de información,*** se describe que conforme a los componentes identificados y el análisis realizado se requiere contemplar unas estructuras de calidad y seguridad para aplicarlos a los componentes y dar robustez a la arquitectura de la información.

"*La construcción de una buena arquitectura de software impacta positivamente sobre su capacidad de satisfacer las necesidades de* ***las partes interesadas****. Cada característica de esta arquitectura (atributos de calidad) es una propiedad medible del sistema que permite evaluar aspectos de calidad tales como la disponibilidad, capacidad de mantenimiento, eficiencia, funcionalidad, seguridad, usabilidad, escalabilidad, facilidad de pruebas, despliegue y desarrollo".*

Alcance del MSPI en Idartes

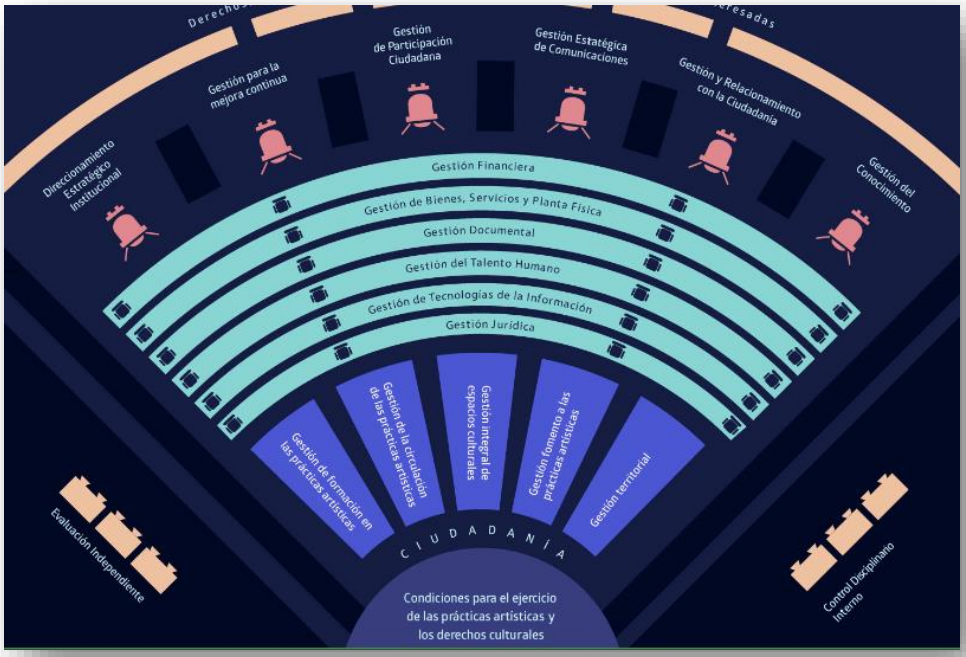
Los objetivos y el alcance del MSPI se deberán reflejar en los objetivos propuestos para el Sistema de Gestión de Seguridad y Privacidad de la Información – SGSI que se pretende implementar en el Idartes. Adicionalmente, los objetivos, el alcance y los límites del SGSI se deberán implementar en esta fase como lo indica el numeral "8.2 Fase de planificación" del documento denominado "Modelo de seguridad y Privacidad de la Información[5]" propuesto por el MinTIC, y lo descrito en la cláusula 1.0 del estándar ISO 27001:2013:

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

"El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad".

Por lo anterior, en estos objetivos se deberían integrar todos los procesos estratégicos, misionales y transversales del Instituto Distrital de Artes - Idartes, y alinear cada uno de los objetivos del MSPI a los objetivos y metas definidas en el Plan Estratégico Institucional.

Ilustración 5. Mapa de Procesos Idartes



Sistema de Gestión de Seguridad de la Información

En el documento "*Plan de Seguridad y Privacidad de la Información 2023",* en el numeral 5. Definiciones, se describe *"Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información en el Idartes, tomando como piloto el proceso de Gestión de Tecnologías de la Información y las Comunicaciones - TIC y que este sea replicado en las unidades de gestión y a los demás procesos y sedes del Instituto, con este documento y su alineación con el Plan Estratégico de Tecnologías de la Información PETI se referencia la estrategia TI y aporta línea de acción apoyando la ejecución de los proyectos, contemplando actualizaciones, para lograr los objetivos estratégicos engranados al Plan Estratégico Institucional y el marco de referencia de arquitectura empresarial del comprender, analizar, construir y presentar, con el enfoque de la estructuración del modelo de gestión Estrategia, Gobierno, Información, Sistemas de Información, Infraestructura de TI, Uso y Apropiación y Seguridad*".

6.2.2.2 Liderazgo y compromiso

El Liderazgo[6] 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 Idartes. A continuación, se describirán, las principales actividades evidenciadas durante el desarrollo de la auditoría:

En el numeral *"6.1 Compromiso de la dirección general" del documento denominado "Políticas de Seguridad de la Información (GTI-POL-02 v4)"* se evidencia que la dirección general a través del Comité Institucional de Gestión y Desempeño de Instituto Distrital de las Artes es la responsable de la aprobación y de realizar el seguimiento a la estrategia de la implementación de la política de seguridad de la información, así como la de comunicar a la organización la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua conforme a los objetivos estratégicos de la entidad.

El Programa de la Auditoría Interna del MSPI fue presentando por el Área de Control Interno y aprobado por el Comité Directivo de Idartes, reunión de apertura realizada el 17 de julio de 2023.

Políticas de seguridad y privacidad de la información.

Durante el desarrollo de la auditoría se evidenció que Instituto Distrital de Artes cuenta con un documento denominado "P*olíticas de Seguridad de la Información (GTI-POL-02 v4)",* publicado el 20 de septiembre de 2021, con la aprobación del jefe de la Oficina Asesora de Planeación y Tecnologías de la Información de Idartes.

El lineamiento trazado en este documento se describe que "*Esta política debe ser aplicada por todos los (as) funcionarios (as), contratistas, proveedores, consultores y todo personal externo que utilice los servicios informáticos que ofrece la entidad, deben conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional. Esta política se actualizará por parte de la Oficina Asesora de Planeación y Tecnologías de la Información, de acuerdo con las disposiciones legales, técnicas o institucionales que defina el Estado colombiano, el Distrito Capital y/o el Instituto Distrital de las Artes – Idartes", sin embargo, durante las (22) sesiones de auditorías el documento no es conocido por todas las partes interesadas.*

En el numeral 6.8 se describe la "Gestión de la Política de Seguridad de la Información, que busca brindar apoyo y orientación a la Dirección General con respecto a la seguridad de la información, de acuerdo con los requisitos legales y normativos del Instituto.

[6] *Se encuentra descrito en la cláusula No. 5 del estándar NTC ISO/IEC 27001:2013*

En el numeral 6.8.1 se describe “La Dirección General debe aprobar el documento de política de seguridad de la información y lo debe publicar y comunicar a todos los funcionarios y partes externas pertinentes”, sin embargo, durante la auditoría no se pudo evidenciar este lineamiento.

En el numeral 6.8.2 se describe “Revisión de la Política de Seguridad de la Información. El documento de la *Política de Seguridad de la Información* se debe revisar mínimo una vez al año o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Durante el desarrollo de la auditoría se evidenció un conjunto de 159 políticas aprobadas por la Oficina Asesora de Planeación y Tecnologías de la Información:

Tabla 2. Relación de políticas encontradas en las Políticas de Seguridad de la Información GTI-POL-02v4

Ítem	Lineamiento
1	6. **RESPONSABILIDADES**
2	6.8. Gestión de la Política de seguridad de la información
3	6.8.1. Documento de la política de seguridad de la información.
4	6.8.2. Revisión de la política de seguridad de la información.
5	6.9. Organización interna
6	6.9.1. Compromiso de la dirección con la seguridad de la información.
7	6.9.2. Coordinación de la seguridad de la información.
8	6.9.3. Acuerdos sobre confidencialidad
9	6.10. Partes externas
10	6.10.1 Identificación de los riesgos relacionados con las partes externas.
11	6.10.2. Consideraciones de la seguridad en los acuerdos con terceras partes
12	7 **GESTIÓN DE ACTIVOS**
13	7.1 Responsabilidad por los activos
14	7.1.1. Inventario de activos
15	7.1.2 Propiedad de los activos
16	7.1.3 Uso aceptable de los activos
17	7.2 Clasificación de la información
18	7.2.1 Directrices de clasificación
19	7.2.2 Etiquetado y manejo de información
20	**8 SEGURIDAD DE LOS RECURSOS HUMANOS**
21	8.1 Antes de la vinculación laboral
22	8.1.1. Roles y responsabilidades
23	8.1.2 Selección
24	8.1.3 Términos y condiciones laborales.
25	8.2 Durante la vigencia del vínculo laboral

26	8.2.1 Responsabilidades de la dirección
27	8.2.2 Educación, formación y concientización sobre la seguridad de la información
28	8.2.3 Proceso disciplinario Control
29	8.3 Terminación o cambio de la contratación laboral
30	8.3.1 Responsabilidades en la terminación
31	8.3.2 Devolución de activos
32	**9. SEGURIDAD FÍSICA Y DEL ENTORNO**
33	9.1 Áreas seguras
34	9.1.1 Perímetro de seguridad física
35	9.1.2 Controles de acceso físico.
36	9.1.3 Seguridad de oficinas, recintos e instalaciones.
37	9.1.4 Protección contra amenazas externas y ambientales.
38	9.1.5 Trabajo en áreas seguras.
39	9.1.6 Áreas de carga, despacho y acceso público
40	9.2 Seguridad de los equipos
41	9.2.1 Ubicación y protección de los equipos
42	9.2.2 Servicios de suministro
43	9.2.3 Seguridad del cableado.
44	9.2.4 Mantenimiento de los equipos.
45	9.2.5 Seguridad de los equipos fuera de las instalaciones.
46	9.2.6 Seguridad en la reutilización o eliminación de los equipos.
47	9.2.7 Retiro de activos
48	10 **GESTIÓN DE COMUNICACIONES Y OPERACIONES**
49	10.1 Procedimientos operacionales y responsabilidades
50	10.1.1 Documentación de los procedimientos de operación
51	10.1.2 Gestión del cambio.
52	10.1.3 Distribución de funciones.
53	10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación.
54	10.2 Gestión de la prestación del servicio por terceras partes
55	10.2.1 Prestación del servicio
56	10.2.2 Monitoreo y revisión de los servicios por terceras partes
57	10.3 Planificación y aceptación del sistema
58	10.3.1 Gestión de la capacidad.
59	10.3.2 Aceptación del sistema.
60	10.4 Protección contra códigos maliciosos y móviles
61	10.4.1 Controles contra códigos maliciosos.
62	10.5 Respaldo
63	10.5.1 Respaldo de la información.
64	10.6 Gestión de la seguridad de las redes
65	10.6.1 Controles de las redes.

66	10.6.2 Seguridad de los servicios de la red.
67	10.7 Manejo de los medios
68	10.7.1 Gestión de los medios removibles
69	10.7.2 Eliminación de los medios.
70	10.7.3 Lineamientos para el manejo de la información.
71	10.7.4 Seguridad de la documentación del sistema.
72	10.8 Intercambio de la información
73	10.8.1 Políticas y procedimientos para el intercambio de información
74	10.8.2 Acuerdos para el intercambio
75	10.8.3 Medios físicos en tránsito.
76	10.8.4 Mensajería electrónica.
77	10.8.5 Sistemas de información del negocio.
78	10.9 Servicios de comercio electrónico
79	10.9.1 Comercio electrónico
80	10.9.2 Transacciones en línea
81	10.9.3 Información disponible al público
82	10.10 Monitoreo
83	10.10.1 Protección de la información del registro
84	10.10.2 Registros del administrador y del operador
85	10.10.3 Registro de fallas
86	10.10.4 Sincronización de relojes
87	11 **CONTROL DE ACCESO**
88	11.1 Requisito del negocio para el control de acceso
89	11.1.1 Lineamientos de control de acceso
90	11.2 Gestión del acceso de usuarios
91	11.2.1 Registro de usuarios.
92	11.2.2 Gestión de privilegios.
93	11.2.3 Gestión de contraseñas para usuarios.
94	11.2.4 Revisión de los derechos de acceso de los usuarios.
95	11.3 Responsabilidades de los usuarios
96	11.3.1 Uso de contraseñas.
97	11.3.2 Equipo de usuario desatendido.
98	11.3.3 Lineamientos de escritorio despejado y de pantalla despejada
99	11.4 Control de acceso a las redes
100	11.4.1 Política de uso de los servicios de red.
101	11.4.2 Autenticación de usuarios para conexiones externas.
102	11.4.6 Control de conexión a las redes.
103	11.4.7 Control de enrutamiento en la red.
104	11.5 Control de acceso al sistema operativo
105	11.5.1 Procedimientos de ingreso seguros

106	11.5.2 Identificación y autenticación de usuarios.
107	11.5.3 Sistema de gestión de contraseñas.
108	11.5.4 Uso de las utilidades del sistema
109	11.5.5 Tiempo de inactividad de la sesión
110	11.6 Control de acceso a las aplicaciones y a la información
111	11.6.1 Restricción de acceso a la información
112	11.6.2 Aislamiento de sistemas sensibles.
113	11.7 Computación móvil y trabajo remoto
114	11.7.1 Computación y comunicaciones móviles.
115	11.7.2 Trabajo remoto.
116	12 **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**
117	12.1 Requisitos de seguridad de los sistemas de información
118	12.1.1 Análisis y especificación de los requisitos de seguridad
119	12.2 Procesamiento correcto en las aplicaciones
120	12.2.1 Validación de los datos de entrada y salida.
121	12.3 Controles criptográficos
122	12.3.1 Política sobre el uso de controles criptográficos.
123	12.3.2 Gestión de llaves.
124	12.4 Seguridad de los archivos del sistema
125	12.4.1 Control del software operativo.
126	12.4.2 Protección de los datos de prueba del sistema.
127	12.4.3 Control de acceso al código fuente de los programas
128	12.5 Seguridad en los procesos de desarrollo y soporte
129	12.5.1 Procedimientos de control de cambios
130	12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo.
131	12.5.3 Restricciones en los cambios a los paquetes de software.
132	12.6 Gestión de la vulnerabilidad técnica
133	12.6.1 Control de vulnerabilidades técnicas
134	13 **GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN**
135	13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información
136	13.1.1 Reporte sobre los eventos de seguridad de la información
137	13.1.2 Reporte sobre las debilidades de la seguridad
138	13.2 Gestión de los incidentes y las mejoras en la seguridad de la información
139	13.2.1 Responsabilidades y procedimientos
140	13.2.2 Aprendizaje debido a los incidentes de seguridad de la información
141	13.2.3 Recolección de evidencia Control
142	14 **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
143	14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio
144	14.1.1 Inclusión de seguridad de la información en el proceso de gestión continuidad del negocio
145	14.1.2 continuidad del negocio y evaluación de riesgos

146	14.1.3 Desarrollo e implementación planes continuidad que incluyen seguridad de la información
147	14.1.4 Estructura para la planificación de la continuidad del negocio
148	14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio
149	15 **CUMPLIMIENTO**
150	15.1 Cumplimiento de los requisitos legales
151	15.1.1 Identificación de la legislación aplicable.
152	15.1.2 Derechos de propiedad intelectual (DPI).
153	1.5.1.3 Protección de los registros de la organización.
154	15.1.4 Protección de los datos y privacidad de la información personal.
155	15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
156	15.2.1 Cumplimiento con las políticas y normas de seguridad.
158	16. **MONITOREO Y SEGUIMIENTO**
159	17. **DECLARACIÓN DE APLICABILIDAD**

Roles y responsabilidades

El MSPI propuesto por el MinTIC, indica que las "*entidades deben definir internamente las responsabilidades*"[7] 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 el Instituto.

La gestión del riesgo se desarrolla bajo el esquema de líneas de defensa, modelo de control que establece y clasifica los roles y responsabilidades de todos los actores del riesgo, para proporcionar aseguramiento de la gestión y prevenir la materialización de los riesgos. Los roles establecidos son:

- *Línea Estratégica*. Alta Dirección.
- *Primera Línea de Defensa*. Responsable del proceso de TI.
- *Segunda Línea de Defensa*. Oficina Asesora de Planeación y Tecnologías de la Información.
- *Tercera Línea de Defensa*. Área de Control Interno.

Durante el desarrollo de la auditoría se evidenció que en el numeral "6. Organización de la seguridad de la información" del documento "Políticas de Seguridad de la Información", relaciona los responsables para la seguridad de la información de Idartes, así:

- Compromiso de la Dirección General
- Compromiso Comité Institucional de Gestión y Desempeño del Idartes
- Compromiso Área de Control Interno
- Compromiso de la Oficina Asesora de Planeación y Tecnologías de la Información

[7] *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*

- Responsabilidades de los propietarios de la información (funcionarios, contratistas y otros terceros).

Sin embargo, los numerales "3.2.1.4. Política de seguridad digital de MIPG[8]" y "7.2.3 Roles y responsabilidades[9]" 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[10]":

Ilustración 6. Captura de pantalla del numeral "3.2.1.4. Política de seguridad digital" de MIPG

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.

6.2.2.3 Planeación

El Modelo de Seguridad y Privacidad de la Información - MSPI establece que, en esta etapa, se debe realizar la identificación de los activos de información, sobre los cuales se debe hacer la identificación, evaluación y tratamiento de los riesgos[11] de Seguridad y Privacidad de la Información del Instituto Distrital de Artes.

Durante el desarrollo de la auditoría, se evidenció que el Idartes cuenta con un Plan de Tratamiento de Riesgos (GTI-P-01 v6), el cual se encuentra alineado 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, no se evidenció que Idartes cuente con un manual o procedimiento para la identificación y clasificación de activos de información asociado al proceso de Gestión de TIC, en el que se describan las actividades que se deberán desarrollar en la identificación, clasificación, valoración, y registro de los activos de información que hacen parte de los procesos del Instituto.

---

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

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

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

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

Inventario de Activos de Información en Idartes

Durante el desarrollo de la auditoría no se evidenció un procedimiento para desarrollar el "Inventario y Clasificación de los Activos de Información" en Idartes, sin embargo, se evidenció el documento denominado "Matriz Activos de Información 2022.xlsx", el cual contiene un listado de 2030 activos de información identificados a octubre de 2022.

Ilustración 7. Captura de pantalla Matriz de Activos de Información

2030	4ES-GTIC	Gestión de Tecnologías de Información y la Comunicaciones Tics	4ES-GTIC-PD-04	PROCEDIMIENTO DE MANTENIMIENTO Y DESARROLLO DE SOFTWARE

Valoración de los riesgos de seguridad de la información

La evaluación de riesgos es el núcleo del MSPI que se implementa en el Instituto Distrital de Artes desde el 2021. Es una metodología adecuada que permite minimizar los potenciales riesgos de integridad, confidencialidad y disponibilidad del inventario de activos de información de Idartes. Durante el desarrollo de la auditoría se evidenció que el Instituto cuenta con una Política de Administración del Riesgo (GMC-POL-01, v4) y un Plan de Tratamiento de Riesgos de Seguridad de la Información (GTI-P-01 v6) publicado el 31 de enero de 2023, 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 en el sitio web de Idartes[12] en el archivo "Mapa de riesgos de Seguridad en la Información 2023 versión final.xlsx" la matriz de evaluación de los riesgos de seguridad de la información del proceso de Gestión de Tecnologías de Información y se encuentra completa, es decir, se analizaron los riesgos de confidencialidad, integridad y disponibilidad, por activos o grupos de activos del proceso de Gestión de Tecnologías de la Información".

Se evidenciaron implementados mecanismos de medición para cada uno de los controles propuestos en las matrices revisadas. Estos mecanismos o indicadores permiten identificar si los controles propuestos son suficientes y eficaces, lo que ayudaría a evidenciar si la "zona de riesgo final" pueda 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 y privacidad de la información.

[12] *https://www.idartes.gov.co/es/transparencia/planeacion/mapas-riesgos*

A continuación, se captura del 2do informe de monitoreo de segunda línea de defensa para los riesgos de gestión, corrupción y seguridad de la información, periodo de mayo a agosto de 2023, la matriz de riesgos de seguridad de la información:

Riesgo MSPI-2. Posible afectación reputacional y económica por pérdida de integridad en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia de autenticación en los aplicativos permitiendo el acceso sin credenciales a la información con datos personales almacenados en los sistemas de información. Probabilidad Inherente: Alta.

Control A.18.1.4. Se deben asegurar la protección y privacidad de la información personal tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales

Ilustración 8. Captura de pantalla Matriz de Riesgos MSPI Agosto 2023

Causa Inmediata ¿Cómo?	Tipos de activo de Información	Activo de Información	Causa Raíz/Vulnerabilidad	Amenaza	Descripción del riesgo	Clasificación del riesgo (Seleccionar)	Frecuencia (Seleccionar)		Probabilidad inherente
Pérdida de Integridad	Bases de datos	Bases de datos de los sistemas de información	Ausencia o deficiencia en los sistemas de autenticación de los aplicativos	No se aplican controles permitiendo el acceso sin credenciales a la información almacenada y procesada en los datos de los sistemas de información.	Posible afectación reputacional por pérdida de integridad en las bases de datos generadas por los sistemas de información institucionales debido a la Ausencia o deficiencia en los sistemas de autenticación de los aplicativos permitiendo el acceso sin credenciales a la información almacenada y procesada en las bases de datos de los sistemas de información.	Daños a activos fijos/ eventos externos	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	500	Media
			Ausencia de controles de acceso a edición, modificación y/o eliminación de datos personales	No se aplican controles definidos para los accesos a drive y repositorios y/o propiedad de la información	Posible afectación reputacional y económica por pérdida de integridad en las bases de datos generadas por los sistemas de información institucionales debido a la ausencia o deficiencia de autenticación en los aplicativos permitiendo el acceso sin credenciales a la información con datos personales almacenados en los sistemas de información.	Usuarios, productos y prácticas	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 vecespor año	1000	Alta
	Información	Información en Drive o Unidades de	Ausencia de documentación para lineamiento de entrega de repositorio a las entidades externas	pérdida de la integridad de la información por acceso indebido	Posible afectación reputacional por pérdida de la integridad en la información misional debido a la ausencia de documentación que de lineamientos en materia de acceso a la información misional permitiendo el acceso no autorizado a drive o unidades de almacenamiento.	Fallas tecnológicas	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	10	Baja

Acción Mejora. Realizar la incorporación de controles para el correcto tratamiento de los datos personales en la actualización de la presente vigencia de la Políticas de Seguridad de la Información y la política de desarrollo conforme a los lineamientos de la Resolución 548-2022 del Idartes.

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 Idartes, en el cual se debe registrar la selección de controles, de acuerdo con los riesgos identificados en la evaluación hecha para cada proceso. El resultado de esta actividad es un documento donde se evidencie la selección de controles para cada riesgo identificado, así como la aceptación del dueño del proceso para implementarlos.

El Plan de Seguridad y Privacidad de la Información es un documento aprobado por la dirección en el cual se planifican las actividades que se desarrollan en la fase de implementación del MSPI. Este documento se encontró en el Instituto descrito como "Plan de Seguridad de la Información (GTI-P-02 v5)[13]".

Con respecto al documento denominado "Declaración de Aplicabilidad Anexo A ISO 27001:2013" de Idartes. Durante el desarrollo de la auditoría no se evidenció el documento denominado "Declaración de Aplicabilidad Anexo A ISO 27001:2013" del Instituto, en el cual se expresa que el Idartes tendrá *"…en cuenta los 114 controles agrupados en 35 objetivos de control y 14 dominios en la penúltima versión de esta norma, de los cuales el Instituto Distrital de Artes aplicará los 114 controles del Anexo A para la implementación del SGSI".*

Así mismo, se evidenció que la revisión de este documento se debe hacer anualmente, sin embargo, durante el desarrollo de la auditoría no se encontraron las versiones actualizadas del documento "Declaración de Aplicabilidad" correspondientes a los tres (3) últimos años: 2021, 2022 y 2023.

6.2.2.4 Soporte de Recursos

Competencia, toma de conciencia y comunicación

El Instituto de Artes no cuenta con un programa o plan de capacitación de seguridad y privacidad de la información estructurado. Se evidenciaron algunos cursos presenciales y virtuales específicos de varios temas relacionados con la gestión de seguridad y privacidad de la información, y por el canal de Comunicaciones del Instituto[14] se reciben recomendaciones para mejorar la seguridad y protección de los activos de información. Sin embargo, no se evidenció el cumplimiento de lo indicado en el numeral "12.6 Seguimiento de indicadores", no se conocía en algunos casos la cobertura de sensibilización a funcionarios/contratistas.

6.2.3 Etapa de Operación/Implementación

Durante el desarrollo de la auditoría se evidenció un 8% de avance en esta etapa.

---

[13] Este documento corresponde a la etapa de "operación y/o implementación"
[14] https://comunicarte.idartes.gov.co/

Ilustración 9. Idartes Instrumento MSPI 2 Trimestre 2023 - Etapa de Implementación

COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Implementación	8%	20%

La etapa de operación[15] 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 etapa, se lleva a cabo la implementación de los "controles" para dar cumplimiento al MSPI:

Ilustración 10. Diseño de la etapa de operación del MSPI propuesto por el MINTIC2016

Planificación e implementación

El Modelo de Seguridad y Privacidad de la Información – MSPI exige que en esta etapa se desarrollen dos (2) 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.

[15] *Esta fase se encuentra descrita en la cláusula No. 8 y en el anexo A del estándar NTC ISO/IEC 27001:2013.*

Durante el desarrollo de la auditoría se evidenció que el Plan de Seguridad y Privacidad de la Información (GTI-P-02 v5) fue publicado el 31 de enero de 2023 y no se evidenció avance de la implementación de cada control del MSPI.

El desarrollo de la etapa de operación requiere finalizar las actividades de la etapa anterior, esto es, atender y priorizar los siguientes aspectos para aumentar el nivel de madurez la operación/implementación del MSPI en el Idartes:

- El Instituto Distrital de Artes debe formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en el Idartes, transversal a la entidad y dependiendo de la Dirección General.

- Idartes debe formalizar la asignación de recursos para la implementación del MSPI en el Instituto. El modelo propuesto por el MINTIC, alienado con la norma NTC ISO/IEC 27001:2013, debe 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"*.

- En Instituto debe finalizar con el levantamiento de activos de información en el Instituto 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 etapa 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 del Idartes.

- Idartes debe formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI del Instituto. Como se evidenció, existe un conjunto de políticas descritas en el documento "Políticas de Seguridad y Privacidad de la Información del Instituto Distrital de Artes (GTI-POL-02 v4)", sin embargo, se debe documentar a través de procedimientos, manuales, guías o instructivos en los que se describan los lineamientos para gestionar la seguridad de la información.

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 debe desarrollar en la etapa 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"[16] propuesto por el MinTIC, la cual se encuentra alineada con los controles definidos en el anexo A de la ISO/EIC 27001:2013.

[16] *https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150511_G8_Controles_Seguridad.pdf*

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 el análisis de la evaluación 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. A continuación, se muestra el avance y la efectividad de la gestión de operación/implementación de los controles de los dominios de control del A5 al A18, así:

Ilustración 21. Idartes Instrumento MSPI 2 Trimestre 2023 – Evaluación de Controles Anexo A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	63	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	57	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	53	100	EFECTIVO
A.9	CONTROL DE ACCESO	59	100	EFECTIVO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	52	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	49	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	44	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	46	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54	100	EFECTIVO
A.18	CUMPLIMIENTO	46	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		54	100	EFECTIVO

La efectividad de los controles aplicados en cada uno de los dominios de control A5, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A17 y A18 muestra un nivel de efectividad *"**Efectivo,** los controles se aplican casi siempre y es poco probable la detección de desviaciones. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.*".

Mientras que para los controles del dominio de control A6 Organización de Seguridad de la Información tiene un nivel de escala de efectividad "***Gestionado**, los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente".*

A continuación, en la siguiente ilustración se muestra la brecha de los controles Anexo A del MSPI Idartes con corte al 30 de junio de 2023:

Ilustración 11. Idartes Instrumento MSPI 2 Trimestre 2023 – Brecha de Controles Anexo A

El MSPI propuesto por el MinTIC se encuentra alineado con estándares Internacionales, como la ISO/IEC 27001:2013, el marco de ciberseguridad del NIST9, la ISO/IEC 31000, con el Marco de Referencia de Arquitectura10 de TI, el Modelo Integrado de Planeación y Gestión (MIPG[17]), la Guía12 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.

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 del Idartes.

Durante el desarrollo de la auditoría se evidenció el documento denominado “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (GTI-P-01 v6)”, publicado el 31 de enero de 2023, en el que se evidenciaron las actividades que se desarrollarían en la fase de “implementación” del MSPI en el Instituto.

[17] *https://www.funcionpublica.gov.co/web/mipg*

6.2.4 Etapa de Evaluación de desempeño.

Durante el desarrollo de la auditoría se evidenció un 7% de avance en esta etapa.

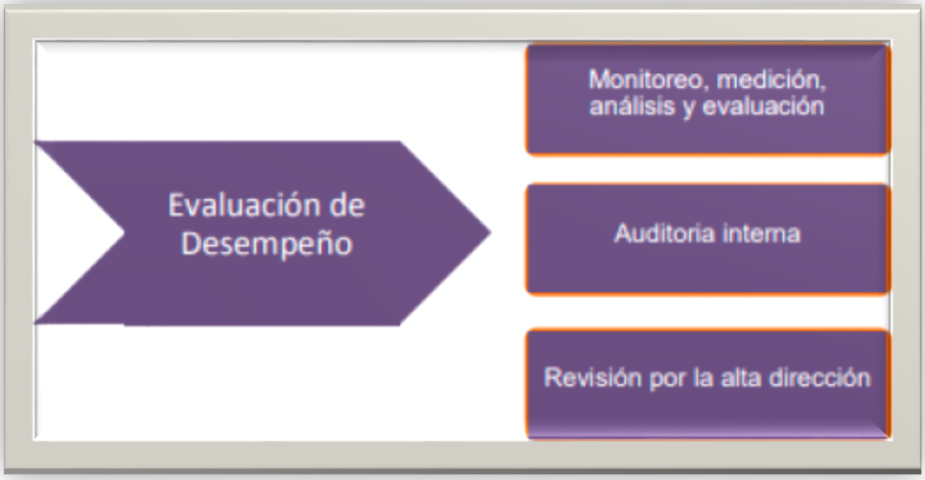
Esta etapa tiene por objetivo la evaluación del desempeño y eficiencia del Modelo de Seguridad y Privacidad de la Información MSPI en el Idartes. Hace parte del "Verificar" en el ciclo PHVA (Planear-Hacer-Verificar- Actuar). Durante el desarrollo de la auditoría se evidenció un avance del 7% en esta etapa:

Ilustración 12. Idartes Instrumento MSPI 2 Trimestre 2023 - Etapa Evaluación de desempeño

COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Evaluación de desempeño	7%	20%

El siguiente es el esquema propuesto por el MinTIC para el desarrollo de esta etapa:

Ilustración 13. Diseño de la etapa de Evaluación de Desempeño del MSPI propuesto por el MINTIC2016



Monitoreo, medición, análisis y avaluación

Durante el desarrollo de la auditoría no se evidenciaron indicadores relacionados con la Seguridad y Privacidad de la Información. 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 el Idartes. El Instrumento está desactualizado, algunos enlaces ya no corresponden a las evidencias. A continuación, se presenta evidencia de información desactualizada y que no cumple el principio de la integridad con el enlace:

Ítem	Levantamiento de Información	Evidencia actual
6	Políticas de seguridad de la información formalizada y firmada	https://www.Idartes.gov.co/es/node/17098
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	https://www.Idartes.gov.co/es/node/17097
15	Planes de tratamiento de los riesgos	https://www.Idartes.gov.co/es/node/17097
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	https://www.Idartes.gov.co/es/node/16479
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	https://www.Idartes.gov.co/es/node/17097

Auditorías internas

La evaluación del MSPI se debería hacer a través de auditorías internas, que se sugiere realizar anualmente. Durante el desarrollo de la auditoría se evidenció que esta fue la primera auditoría que se hace al MSPI en el Instituto Distrital de Artes. 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 el Idartes.

De igual manera, el MSPI que se continue implementando en el Instituto deberá ser revisado[18] y aprobado por la Alta Dirección, cuando así se considere, de tal manera que la Dirección podrá evaluar el avance desde la óptica estratégica.

6.2.5 Etapa de Mejora Continua

Esta fase tiene por objetivo la consolidación de los resultados de la etapa de “Evaluación de desempeño” en el documento denominado “Plan de Mejora Continua” relacionado con el Modelo de Seguridad y Privacidad de la Información en el Idartes. Esta etapa hace parte del “Actuar” en el ciclo PHVA (Planear-Hacer-Verificar- Actuar) y se evidenció que se lleva un avance del 4% en esta etapa:

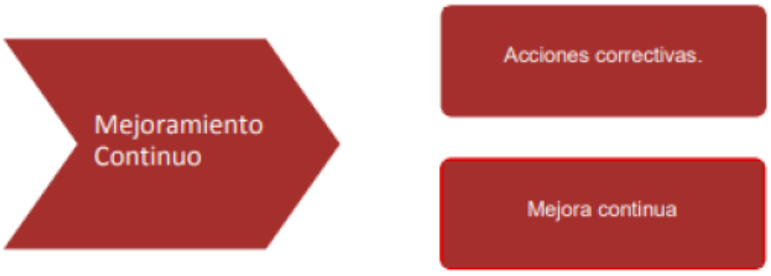
[18] *Las evaluaciones del MSPI deberían ser a intervalos planificados, una sola reunión será suficiente para el cumplimiento de esta actividad.*

Ilustración 14. Idartes Instrumento MSPI 2 Trimestre 2023 - Etapa Mejora Continua

COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Mejora continua	6%	20%

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

Ilustración 15. Diseño de la etapa de Mejoramiento Continuo del MSPI propuesto por el MINTIC2016



El desarrollo del plan de mejora continua del MSPI en el Instituto 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 hacer evaluación o seguimiento al MSPI.

6.3 FASE 3. Auditoría de Gestión de Protección de Datos Personales

Se determina el estado actual y el nivel de madurez de la protección de datos personales en Idartes mediante la aplicación de la herramienta de la Secretaría Jurídica Distrital de la Alcaldía Mayor de Bogotá, basada en el marco del Programa Integral de Protección de Datos Personales, que tiene el propósito de definir los lineamientos y procedimientos para la implementación, monitoreo, sostenimiento y mejora continua, dando cumplimiento al compromiso institucional de proteger la información personal que se custodia en la entidad y dando cumplimiento a la Ley 1581 de 2012 y sus decretos reglamentarios.

De acuerdo con las resoluciones 160 de 2017 y 874 de 2020, se adopta el manual de política de seguridad del sitio web en materia de datos personales y protección de datos personales recaudados en las bases de datos creadas en entidad y se actualiza la Política de Protección de Datos Personales en el Idartes y se adoptan los formatos de autorización de tratamiento de datos personales y el aviso de privacidad de la entidad.

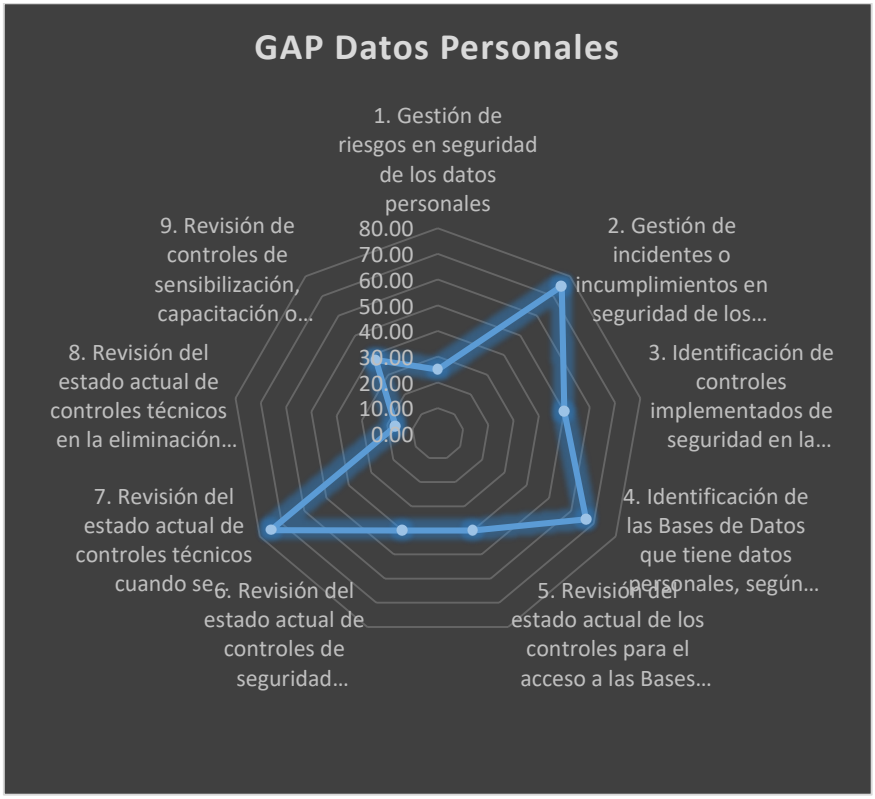
En el mes de agosto de 2023 los encargados de la gestión de seguridad y privacidad de la información de las áreas de Tecnologías de la Información y Jurídica, diligenciaron el checklist de revisión de los controles de seguridad de la información correspondiente a la Protección de Datos Personales – Instrumento propuesto por la Secretaría Jurídica de la Alcaldía Mayor de Bogotá, obteniendo el siguiente resultado:

Tabla 3. Matríz de diagnóstico de Protección de Datos Personales – Idartes Ago.2023

Nivel de Madurez Agosto 2023	
1. Gestión de riesgos en seguridad de los datos personales	25.00
2. Gestión de incidentes o incumplimientos en seguridad de los datos personales	75.00
3. Identificación de controles implementados de seguridad en la captura de la información de datos personales.	50.00
4. Identificación de las Bases de Datos que tiene datos personales, según el alcance establecido a nivel de procesos y sistemas de información.	66.67
5. Revisión del estado actual de los controles para el acceso a las Bases de datos con información personales.	40.00
6. Revisión del estado actual de controles de seguridad implementados en el almacenamiento de los datos personales (Ejemplo: Cifrado, acceso, entre otros).	40.00
7. Revisión del estado actual de controles técnicos cuando se comparte la información de datos personales con terceras partes.	75.00
8. Revisión del estado actual de controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos.	16.67
9. Revisión de controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales.	37.50
Medicion	425.83
Avance %	**47.31**

Del análisis de la información de resultado en la matriz anterior, se visualiza una oportunidad al revisar los controles asociados a la gestión de riesgos de seguridad de los datos personales, los controles técnicos en la eliminación de datos personales o cuando pasan a ser históricos y por último, pero no menos importante los relacionados con los controles de sensibilización, capacitación o formación a los servidores públicos en lo relacionado con protección de datos personales.

Ilustración 16. GAP Análisis de la Protección de Datos Personales – Idartes Ago.2023



6.4 FASE 4. Auditoría de Gestión de Ciberseguridad

Como parte del diagnóstico se aplicó la herramienta del BID, ya que la misma se basa en el marco de ciberseguridad de la NIST que se encuentra en el MSPI. Este diagnóstico se realizó a partir de la información suministrada por el equipo auditado de la Oficina Asesora de Planeación y Tecnologías de la Información el 8 de septiembre de 2023. Los resultados se recogen en la siguiente tabla. Se utilizó la herramienta de Autoevaluación en Ciberseguridad disponible en el siguiente enlace: https://www.iadb-tools.org/

Tabla 4. Diagnóstico BID 2023

Identificar	Proteger	Detectar	Responder	Recuperar
77%	66%	75%	55%	77%

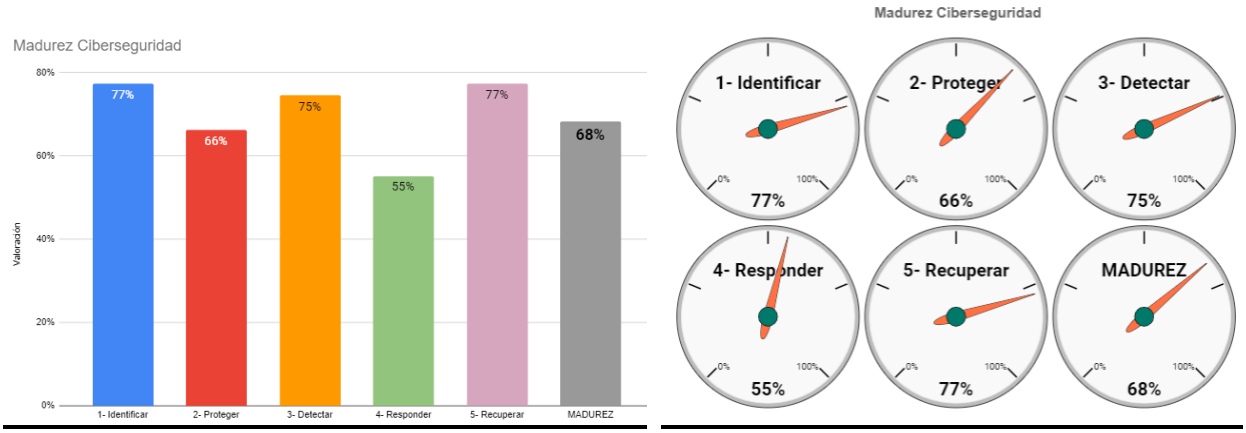


Ilustración 17. Nivel de madurez Ciberseguridad

DOMINIO	Madurez
1- Identificar	77%
2- Proteger	66%
3- Detectar	75%
4- Responder	55%
5- Recuperar	77%
MADUREZ	68,3%

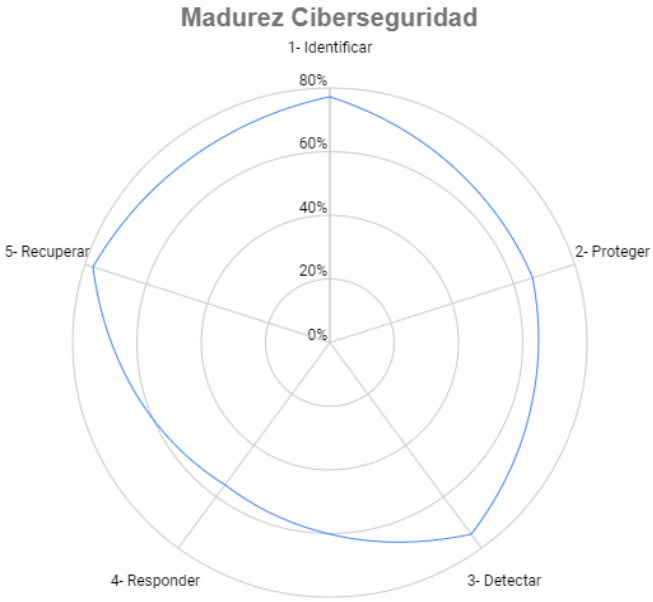


Tabla 5. Diagnóstico Ciberseguridad IDARTES

Las recomendaciones brindadas por la herramienta se detallan a continuación:

Dominio 1 - IDENTIFICAR:

Gobernanza: La gobernanza de la seguridad de la información permitirá a la entidad tener los riesgos manejados y aceptados dentro de los niveles requeridos.

Por lo que se recomienda: Adoptar el Modelo de Seguridad y Privacidad de Información

- El MSPI le permite a una entidad definir políticas y procesos para gestionar de manera eficiente la seguridad de la información.

- Definir la Política de Seguridad de la Información, comunicarla a todo el personal de la entidad, definir las políticas relacionadas, los procesos que garanticen el cumplimiento y los procedimientos que desarrollen como y quienes deben realizar las distintas actividades.
- Definir el comité de Seguridad de la Información, el mismo debe estar conformado al menos por el responsable de seguridad de la Información (CISO, CSO), representantes de las distintas direcciones de la entidad, abogados, encargados de las comunicaciones, entre otros.
- En el caso particular de organismos gubernamentales, es importante que en el mismo se cuente con la participación del gobierno central y/o agencia rectora de la seguridad del país.
- Definir los objetivos estratégicos de Seguridad de la Información.
- Analizar el impacto que tiene en la entidad las normativas que pueden aplicar. En particular, se debe revisar las leyes de protección de datos personales y aquellas que apliquen según los activos administrados.

Evaluación de riesgos: La seguridad es un proceso de mejora continua, las organizaciones deben tener claro las expectativas de seguridad de la información. Si lo llevamos a términos más formales y cuantificables, las organizaciones deben elegir el nivel de riesgo que están dispuestos a aceptar y llevar a cabo una adecuada gestión de riesgos para lograr los objetivos.

Por lo que se recomienda: Definir políticas, proceso y procedimientos de gestión de vulnerabilidades en los activos críticos de Información, el cual debe incluir como mínimo: la identificación de sus vulnerabilidades y amenazas, la recepción de información de diferentes fuentes, ejecuciones periódicas de hackeos éticos para su posterior evaluación y análisis de amenazas (desde fuentes internas y externas).

Definir la probabilidad de ocurrencia de las distintas amenazas y para cada una de ellas analizar el impacto potencial en el negocio. Definir los controles a aplicar con el objetivo de mitigar los potenciales impactos y lograr un nivel de riesgo residual aceptable.

Estrategia para la gestión de riesgos: La entidad debe tener un plan de tratamiento de riesgos, el mismo debe ser comprendido y aprobado por el comité de seguridad de la información en conjunto con la dirección o alta gerencia.

Por lo que se recomienda:

- Definir un proceso de gestión de riesgos, el cual debe tener definido los umbrales de tolerancia del riesgo que la organización está dispuesta asumir.
- Definir la Política de gestión y comunicarla a todos los interesados.

Dominio 2 - PROTEGER:

Concientización y formación: Las organizaciones deben tener su política de seguridad de la información, pero si la misma no es familiar para la organización no será útil al momento de garantizar que se cumplan con los requisitos y objetivos de seguridad. Por otro lado, se pueden tener muchas herramientas técnicas que apoyen y faciliten las medidas de seguridad, pero siempre se tiene al usuario final como un punto de falla para cualquier control a implementar.

Por lo que se recomienda:

- Implementar un programa de concientización, en donde los interesados comprendan y analicen los distintos aspectos de la seguridad de la información, conozcan el valor real de su información y las principales amenazas que están expuestos.
- Implementar programas particulares de concientización para los usuarios que tienen privilegios o realizan tareas con impacto mayor a la entidad.
- Definir programas de capacitaciones y formación especializada en seguridad para los responsables de administrar los activos críticos de la entidad, de desarrollar tareas específicas de seguridad como por ejemplo respuesta a incidentes. Es importante que su accionar sea rápido, sistematizado y eficiente con el fin de minimizar el impacto.

Procesos y procedimientos para la protección de la información: Se deben definir procesos y procedimientos que garanticen la protección de los activos de Información.

Por lo que se recomienda:

- Definir proceso de gestión de cambios el cual debe incluir la línea base de las configuraciones de los sistemas.
- Implementar un ciclo de desarrollo de sistemas e incorporar actividades de seguridad al mismo, esto aplica a la institución tenga desarrollos a medida.
- Definir la Política de backup de la organización, en el cual se defina y se mantenga los lineamientos de los respaldos y las responsabilidades asociadas. Los mismos deben ser testeados en forma periódica con el fin de garantizar su correcto funcionamiento.
- Definir Política, procesos y procedimientos de destrucción de información y activos.
- Definir e implementar controles medioambientales en centros de datos y áreas relacionadas, por ejemplo: temperatura, humedad, entre otros.

Tecnología de protección: Es importante implementar tecnologías de protección o seguridad adecuadas para los activos de la organización.

Por lo que se recomienda:

- Definir políticas, procesos y procedimientos de manejo de logs de los activos (aplicaciones, sistemas operativos, equipamiento de red, etc.).
- Implementar un sistema que permita el manejo de logs de los activos de manera estandarizada y centralizada.

Dominio 4 - RESPONDER:

Planificación de la respuesta: Las organizaciones deben estar preparadas para dar una correcta respuesta ante la detección de un evento de seguridad.

Por lo que se recomienda:

- Definir los roles y las responsabilidades de los distintos interesados tanto sea internos o externos a la organización.
- Definir las políticas, procesos y procedimiento para dar respuesta ante un incidente de seguridad.
- Comunicar la Política a todos los usuarios de la organización e incluirlo en el plan de capacitación de la organización.

Mejoras en respuesta: Durante la respuesta a un incidente el equipo técnico se enfrenta a nuevos ataques y busca posibles acciones de mitigación en función de los efectos que vayan surgiendo. Este proceso es constante y de aprendizaje en cada una de las acciones, ya que es difícil encontrar dos situaciones con el mismo comportamiento.

Por lo que se recomienda: Incorporar las lecciones aprendidas al proceso y procedimientos de respuesta ante incidentes.

Dominio 5 - RECUPERAR:

Planificación de la recuperación: Las organizaciones deben estar preparadas para recuperarse luego de la ocurrencia de un incidente de seguridad de la información. Para el caso particular de organismos gubernamentales, se debe definir y analizar cómo sería el plan de recuperación de los servicios a los ciudadanos y aquellos críticos que sirven de apoyo a otras organizaciones gubernamentales o privadas tomando posibles escenarios, como ser la interrupción del servicio de red, corrupción de la información, entre otros.

Por lo que se recomienda:

- Definir los planes de recuperación de los servicios críticos de la organización. Estos planes deben contener las políticas, procesos y procedimientos requeridos que definan el accionar de las personas, el uso de las herramientas y los recursos necesarios. Todo lo antes mencionado con el objetivo de dejar operativos los servicios en un tiempo previamente estipulado. Para cada uno de los posibles escenarios se deberá definir un plan de acción, escribir los procedimientos asociados y establecer qué servicios se recuperarán y en qué condiciones. Es importante aclarar que este es un estado transitorio, por lo que se pueden acordar niveles de calidad inferiores hasta restablecer las condiciones normales.
- Definir instancias de simulación de los procedimientos para su validación.
- Incorporar los procedimientos en el plan de capacitaciones de los usuarios privilegiados.

Comunicaciones: Se debe contar con un plan de comunicación ante la necesidad de recuperación de un servicio, es crucial para su eficacia tomar acciones en forma rápida y oportuna, por lo que se debe contar con los canales de comunicaciones con los distintos actores involucrados en forma previa.

Por lo que se recomienda:

- Definir el plan de comunicaciones ante la afectación de un servicio crítico, en donde se define quienes son los interlocutores válidos y los mecanismos de comunicación.
- Establecer acuerdos para el apoyo por parte de otras entidades gubernamentales, centros especializados en seguridad (CERT, CSIRT, etc.), proveedores de servicio, por lo que se debe contar con acuerdos que permitan desarrollar las actividades requeridas en forma coordinada.
- Definir el plan de comunicaciones con el ciudadano, estas deben estar acordes a la reglamentación vigente y aplicable a la organización. En la misma se detalla cuando la organización debe comunicar y establecer los tiempos para hacerlo.

7. RESULTADOS

Producto de la evaluación realizada, se presentan los siguientes resultados:

Tabla 6. Relación de Resultados de la Auditoría Interna

Tipo de Resultado	Cantidad	Referenciación
Fortalezas	2	FO01, FO02
Cumplimientos	4	CU01, CU02, CU03 y CU04
Incumplimientos	1	IN01
Oportunidades de Mejora	8	OM01, OM02, OM03, OM04, OM05, OM06, OM07 y OM08
Total	**15**	

7.1 FORTALEZAS

FO01. **Liderazgo y compromiso**

La alta dirección demuestra liderazgo y compromiso con respecto al Modelo de Seguridad y Privacidad de la Información, promueve la mejora continua y soporta otros roles relevantes de gestión para demostrar su liderazgo según aplique a sus áreas de responsabilidad. (Requerimiento de norma 5.1).

FO02. Política de Seguridad y Privacidad de la Información

La alta dirección establece la Política de Seguridad y Privacidad de la Información, la cual está disponible como información documentada, se comunica dentro del Instituto y está disponible a las partes interesadas. (Requerimiento de norma 5.2).

7.2 CUMPLIMIENTOS

CU01. Acciones para atender riesgos y oportunidades

En la planeación del modelo de seguridad y privacidad de la información, se determinan los factores externos e internos relevantes para sus fines y que afectan su capacidad de lograr los resultados esperados, así como determinar las partes interesadas que son relevantes al Sistema de Gestión de Seguridad de la Información. (Requerimiento de norma 6.1.1).

CU02. Evaluación del riesgo en seguridad de la Información

La entidad define y aplica la evaluación completa del riesgo de seguridad de la información al proceso de Gestión de Tecnologías de la Información, evalúa las potenciales consecuencias y determina los niveles de riesgos, priorizando el tratamiento de riesgo para los riesgos analizados. (Requerimiento de norma 6.1.2).

CU03. Tratamiento de los riesgos en seguridad de la información

La entidad define y aplica el proceso de tratamiento de riesgos de Seguridad de la Información en el proceso de Gestión de Tecnologías de la Información, considerando los resultados de la evaluación de riesgos y determinando los controles necesarios para implementar opciones pertinentes y formular el plan de tratamiento de riesgos MSPI. (Requerimiento 6.1.3).

CU04. Aspectos de seguridad de la información de la gestión de continuidad del servicio de TI

La entidad establece la inclusión de un plan de continuidad TI que fortalece la planificación, implementación, evaluación y mejora del MSPI, que permite garantizar la restauración oportuna de las operaciones esenciales. La correcta implementación de la gestión de la continuidad del servicio de TI disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, Idartes estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por un incidente.

7.3 INCUMPLIMIENTOS

IN01. Tratamiento de los riesgos en seguridad de la información

El MSPI no está generando la Declaración de Aplicabilidad – SOA, la cual contiene los controles necesarios para implementar las opciones escogidas de tratamiento de riesgos en seguridad de la información y una justificación para la exclusión de controles del Anexo A. Documento firmado por alta dirección. (Requerimiento 6.1.3 d)

7.4 OPORTUNIDADES DE MEJORA

OM01. Planificación

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 pretende fortalecer la implementación en Idartes, de tal manera que se integren los procesos misionales, estratégicos y transversales, de acuerdo con lo propuesto en el numeral "8.2 Fase de planificación" del documento denominado "Modelo de Seguridad y Privacidad de la Información[19]" propuesto por el MINTIC y lo descrito en la cláusula 1.0 del estándar ISO 27001:2013.

OM02. Plan de capacitación, sensibilización y comunicación

Desarrollar e integrar un esquema de conocimiento y capacidades institucional para la cultura de la gestión de seguridad y privacidad de la Información con la participación activa de la Alta Dirección para la vigencia 2023, en el cual se debería involucrar de manera activa al Área de Comunicaciones y la Gestión de Talento Humano, para efectos de evidenciar la participación de la totalidad de funcionarios / contratistas de Idartes.

OM03. Integrar el MSPI al Sistema Integrado de Gestión – SIG y el Modelo Integrado de Planeación y Gestión - MIPG

A través del Decreto 591 de 2018 Idartes realizó la modificación del Sistema Integrado de Gestión Distrital (SIG) bajo los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG-, fortaleciendo los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto, sin embargo, hay una oportunidad de mejora para integrar la estrategia de la seguridad y privacidad de la información institucional del MSPI y re potencializar la gestión integral del talento humano, agilizar las operaciones, fomentar el desarrollo de una cultura organizacional sólida, promover la participación y confianza de la ciudadanía.

OM04. 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 el Instituto Distrital de Artes, trasversal a la entidad y dependiendo de 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

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

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[20]".

OM05. 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 el Idartes, de acuerdo con los dispuesto en la fase 4 "Evaluación y desempeño", con el objetivo de medir el desempeño y eficiencia de los requerimientos y controles de MSPI.

OM06. Auditorías internas de gestión

Se sugiere incluir en el Plan Anual de Auditoría (PAA) la evaluación anual del Modelo de Seguridad y Privacidad de la Información – MSPI que se pretende implementar/operar en el Idartes, esto con el objetivo de dar cumplimiento a lo dispuesto en la fase 4 "Evaluación y desempeño" del MSPI.

OM07. Formalizar procesos, guías e instructivos del MSPI

Se sugiere formalizar los procedimientos de cada una de las actividades desarrolladas en el MSPI del Instituto. Como se evidenció, existe un conjunto de políticas descritas en el documento "Políticas de Seguridad y Privacidad de la Información del Idartes", 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 y Privacidad de la Información del Instituto.

OM08. Actualización permanente del Instrumento MSPI

Se sugiere mantener actualizado el Instrumento MSPI como la herramienta de diagnóstico del Instituto en materia de seguridad y privacidad de la información que permita obtener un resultado preciso y oportuno en la construcción y mejora de los procesos de transformación digital necesarios y requeridos para atender los cambios culturales estratégicos, tácticos y operativos de la entidad, así como para el desarrollo de nuevas capacidades frente a las vulnerabilidades del entorno digital que puedan afectar los activos de información del Idartes en su principios de confidencialidad, disponibilidad e integridad.

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

8. CONCLUSIÓN

Soportados en la documentación del Instrumento MSPI de 2018 a 2023 suministrados por el Instituto se puede indicar frente a la madurez del Modelo de Seguridad y Privacidad de la Información – MSPI que éste ha mostrado avances graduales en términos de conformidad con la norma ISO/IEC 27001. Sin embargo, se observa que la implementación y maduración del MSPI ha sido lenta y ha enfrentado numerosos desafíos, incluyendo la falta de recursos, roles y funciones poco claras, y la falta de una cultura de seguridad de la información en toda la entidad.

A partir de 2021, se observa una mejora en la gestión y control de la seguridad de la información, aunque siguen existiendo áreas por mejorar, especialmente en lo que se refiere a la actualización y precisión de la información documentada y a la asignación de roles y responsabilidades a los funcionarios y partes interesadas involucradas.

Finalmente, a pesar de los avances observados, el Instituto necesita seguir haciendo esfuerzos considerables para continuar fortaleciendo el MSPI y estar articulado con los demás instrumentos institucionales. Así mismo, por la actual situación de los ataques cibernéticos, es crucial que la alta dirección se involucre más activamente y asuma la responsabilidad de dirigir y apoyar la implementación y operación del Modelo de Seguridad y Privacidad de la Información MSPI.

9. RECOMENDACIONES

1. Fortalecer e incrementar la madurez del Modelo de Seguridad y Privacidad de la Información MSPI, ampliando el alcance del MSPI a todos los procesos del Instituto Distrital de las Artes – Idartes.

2. Mejorar la gobernanza y formalización de la gestión de Seguridad de la Información, Protección de Datos Personales y la Ciberseguridad. Se sugiere formalizar el rol y las funciones del responsable de la Seguridad y Privacidad de la Información en el Instituto, trasversal a la entidad y dependiendo de la Dirección General.

3. Desarrollar e integrar un esquema de conocimiento y capacidades institucional para la cultura de la gestión de seguridad y privacidad de la Información con la participación activa de la Alta Dirección para la vigencia 2023, en el cual se debería involucrar de manera activa al Área de Comunicaciones y la Gestión de Talento Humano, para efectos de evidenciar la participación de la totalidad de funcionarios / contratistas de Idartes.

4. 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 el Instituto Distrital de las Artes, esto con el objetivo de dar cumplimiento a lo dispuesto en la fase 4 “Evaluación y desempeño” del MSPI.

5. Integrar la estrategia de la seguridad y privacidad de la información - MSPI al Sistema Integrado de Gestión Distrital (SIG) y el Modelo Integrado de Planeación y Gestión - MIPG para fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto, re potencializar la gestión integral del talento humano, agilizar las operaciones, fomentar el desarrollo de una cultura organizacional sólida, promover la participación y confianza de la ciudadanía.

6. Probar este año el plan de continuidad TI que fortalezca la planificación, implementación, evaluación y mejora del MSPI, garantizando la restauración oportuna de las operaciones esenciales. Así mismo, como la correcta implementación de la gestión de la continuidad del servicio de TI, que disminuya la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, Idartes estaría preparada para responder en forma adecuada y oportuna de un daño potencial que pueda ser ocasionado por un incidente.

Elaboró	**Aprobó**
NOMBRE Y APELLIDO Cargo: /Contratista	**NOMBRE Y APELLIDO** Asesor/a control interno