Bogotá D.C, diciembre 19 de 2024

PARA: MARIA CLAUDIA PARIAS DURÁN
Directora General

DE: NESTOR FERNANDO AVELLA AVELLA
Jefe de Control Interno (e)

ASUNTO: Remisión del Informe final de auditoría interna MSPI Procesos del Idartes.

Cordial saludo, Directora:

En desarrollo del plan anual de auditoría 2024 versión 4 del Instituto Distrital de las Artes y en cumplimiento del Decreto 648 de 2017 en el rol de evaluación y seguimiento, que deben desempeñar las oficinas de control interno o quien haga sus veces, así como del Decreto N°984 del 14 de mayo de 2012, por el cual se modifica el Art. 22 del Decreto N°1737 de 1998, se remite el informe final de la auditoría interna al Modelo de Seguridad y Privacidad de la Información – MSPI Procesos del Idartes, cuyo objetivo correspondió a “Evaluar la gestión del Modelo de Seguridad y Privacidad de la Información – MSPI”, mediante la auditoría interna, teniendo como referente el modelo MSPI y la norma NTC ISO/IEC 27001:2013.

Cordialmente,

NESTOR FERNANDO AVELLA AVELLA
Jefe de Control Interno (e)

Proyectó: CLARA PATRICIA MUÑOZ JIMÉNEZ. Contratista Oficina Control Interno.
Documento 20241300731103 firmado electrónicamente por:

NESTOR FERNANDO AVELLA AVELLA, Asesor Control Interno (e), Área de Control Interno, Fecha firma: 20-12-2024 13:38:58

Revisó: CLARA PATRICIA MUNOZ JIMENEZ - Contratista - Área de Control Interno

Anexos: 1 folios

293d8f1656852ef60d3c0493264cd41b08f9b230c3e6deb90ca17dbdb1825cce
Codigo de Verificación CV: 6150a Comprobar desde:

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

PROCESOS DEL IDARTES

ÁREA DE CONTROL INTERNO

INSTITUTO DISTRITAL DE LAS ARTES

BOGOTÁ D.C.

DICIEMBRE DE 2024

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 2024 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 Procesos*** del Idartes***,*** 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. Así mismo, 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

Evaluar la gestión del Modelo de Seguridad y Privacidad de la información – MSPI en todos los Procesos del Idartes.

OBJETIVOS ESPECÍFICOS

- Evaluar las medidas de protección (controles) que existen en la entidad, analizar las vulnerabilidades y riesgos existentes, en cumplimiento de las medidas y políticas de seguridad establecidas.
- Analizar las políticas y procedimientos de seguridad definidos y se revisa su grado de cumplimiento.
- Verificar y evaluar el cumplimiento del marco normativo y legal que lo rige.
- Verificar la gestión y los componentes de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación (Líneas de Defensa).

2. ALCANCE

El período a evaluar es el comprendido entre el 01 de enero de 2024 y el 30 de noviembre de 2024, donde se realizará la auditoría interna al Modelo de Seguridad y Privacidad de la Información para los diecinueve (19) procesos del 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 5 de noviembre al 4 de diciembre de 2024.

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

La presente auditoría se desarrolló mediante mesas de trabajo presencial y virtual con los diferentes referentes designados, verificando y constatando el cumplimiento la conformidad de los requisitos normativos acorde a las listas de verificación elaboradas. Se realizó la toma de casos aleatorios y análisis de la información referente a los procedimientos, registros documentales, registros de riesgos, herramientas, entre otros,

Las mesas de trabajo fueron agendadas acorde a la programación establecida, adicionalmente el auditor tuvo en cuenta los siguientes aspectos:

- Revisión de la documentación de seguridad de la información: El auditor solicitó y revisó la documentación existente en la entidad con respecto a la gestión de la seguridad de la información, verificando los documentos de políticas de seguridad de la información, procedimientos, guías, registros de actas entre otros documentos. De la misma manera se revisaron los procesos definidos para determinar la relación con el modelo de seguridad de la información MSPI.

- Consultas con el personal designado**:** El auditor realizó consultas específicas al personal designado de la entidad y consultó piezas comunicativas elaboradas, con el fin de conocer el nivel de concientización frente a la seguridad y privacidad de la información.

4. CRITERIOS

Para el desarrollo de la presente auditoría se tuvo en cuenta la siguiente 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.
- Ley 1915 de 2018. “Por medio de la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.
- 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 de Tecnologías de Información – PETI 2024.
- Plan de Seguridad y Privacidad de la Información 2024.
- Instrumento de evaluación MSPI 2024 - 3 trimestre, 1° de octubre de 2024.
- Política de Seguridad de la Información, versión 6 de 2024
- Plan de tratamiento de riesgos de seguridad y privacidad de la información 2024.
- Las demás normas pertinentes relacionadas con el objetivo de la auditoría.
- Plan Estratégico Institucional 2024-2027.
- Normograma de Idartes. GJU-F-103 v1 23-09-2024

5. RIESGOS DE AUDITORÍA

El riesgo emitir un concepto errado por parte de la auditora designada de esta auditoría se puede configurar, por la entrega de información inoportuna, incompleta, confusa o inexacta.

6. RESULTADOS

El Modelo de Seguridad y Privacidad de la Información también conocido como - MSPI y liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, imparte los lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas en materia de seguridad de la información, tomando como referencia el estándar internacional ISO27001 e ISO27002, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), logrando a su vez la alineación e implementación de la Política de Gobierno Digital - Decreto 1008 de 2018 y su habilitador transversal de seguridad de la información.

La planificación e implementación del Modelo MSPI está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales, tamaño, estructura del Idartes y su objetivo principal consiste en preservar la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Dicho modelo es actualizado periódicamente y recogerá los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Ley de la Propiedad Intelectual, Transparencia y Acceso a la Información Pública, entre otras. El modelo pretende facilitar la construcción de la política de privacidad por parte de la entidad y fija los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos, sistemas de información y las personas vinculadas con la información.

Es importante tener presente que la norma ISO27001:2013 certificable, evalúa el ciclo de vida del sistema de acuerdo con sus 7 dominios y el código de buenas prácticas ISO27002:2013, se evalúa los 14 dominios y sus 114 controles, todos estos elementos descritos hacen parte del instrumento de autoevaluación que el MinTIC exige a cada entidad para conocer el nivel de avance en la implementación del modelo y para efectos del objetivo de la presente auditoria se eligieron algunos de los requisitos para determinar su conformidad.

Entendimiento de necesidades y planeación

El plan de las sesiones híbridas (presenciales y virtuales) de auditoría interna de gestión MSPI, se realizó con los líderes de los Procesos de Idartes y sus equipos de trabajo 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. A continuación, en la siguiente tabla se tiene el Cronograma trazado para llevar a cabo el Plan de Auditoría Interna a los Procesos de Idartes:

Tabla 1. Programación de las Sesiones de Auditoría Interna MSPI PROCESOS

Id	Sesión Auditoría Interna	Fecha	Líder del Proceso
SP01	DIR-C-01 v2 – Direccionamiento Estratégico Institucional	Nov. 5/2024	Jefe Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI
SP02	CEI-C-01 v2 – Evaluación Independiente	Nov. 6/2024	Jefe Oficina Asesora de Control Interno
SP03	GMC-C-01 v4 – Gestión para la Mejora Continua	Nov. 7/2024	Jefe Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI
SP04	GFI-C-01 v3 – Gestión Financiera	Nov. 7y8/2024	Subdirector Administrativo y Financiero
SP05	C-CDI-01 v3 Control Disciplinario Interno	Nov. 12/2024	Jefe Oficina de Control Disciplinario
SP06	GPAC-C-01 v1 Gestión Participación Ciudadana	Nov. 12/2024	Jefe Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI
SP07	GCO-C-3 v5 Gestión del Conocimiento	Nov. 13/2024	Jefe Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI
SP08	GTI-C-01 v2 Gestión de Tecnologías de la Información	Nov. 14/2024	Jefe Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI
SP09	GBS-C-01 v2 Gestión de Bienes, Servicios y Planta Física	Nov. 14/2024	Subdirector Administrativo y Financiero
SP10	GDO-C-01 v3 Gestión Documental	Nov. 18/2024	Subdirector Administrativo y Financiero
SP11	GTH-C-01 v2 Gestión del Talento Humano	Nov. 18/2024	Subdirector Administrativo y Financiero
SP12	GRC-C-01 v3 Gestión y Relacionamiento con la Ciudadanía	Nov. 19/2024	Subdirector Administrativo y Financiero
SP13	SST-C-01 v1 Gestión en Seguridad y Salud en el Trabajo	Nov. 19/2024	Subdirector Administrativo y Financiero
SP14	GJU-C-01 v2 Gestión Jurídica	Nov. 22/2024	Jefe Oficina Asesora Jurídica
SP15	Gestión de Protección de Datos Personales	Nov. 22/2024	Jefe Oficina Asesora Jurídica
SP16	Gestión de Ciberseguridad	Nov. 25/2024	Jefe Oficina Asesora de Planeación y Tecnologías de la Información - OAPTI
SP17	GEC-C-01 v2 Gestión Estratégica de Comunicaciones	Nov. 28/2024	Asesora de Comunicaciones

SP18	Gestión de Protección de la Propiedad Intelectual de Software	Nov. 28/2024	Jefe Oficina Asesora Jurídica
SP19	Gestión Circulación Prácticas Artísticas y Gestión Fomento Prácticas Artísticas	Nov. 28/2024	Subdirectora de las Artes
SP20	GFOR-C-01 v2. Gestión de Formación en las Prácticas Artísticas.	Nov. 28/2024	Subdirectora de Formación Artística – SFA
SP21	GIEC-C-01 v2. Gestión Integral de los Espacios Culturales	Dic.4/2024	Subdirectora Equipamientos Culturales

En el expediente de la auditoría interna MSPI No. 20241000190900006E se tiene registrado en la plataforma de Orfeo las actas de reuniones de cada una de las sesiones de auditoría MSPI Sistemas de Información 2024 realizadas y los soportes correspondientes. A continuación, mediante tablas se representan los resultados obtenidos respecto a los requisitos y controles seleccionados:

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 sigue siendo 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.

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 2024 3Trimestre”, en el cual se evidencia el cumplimiento de esta actividad.

Ilustración 2. Idartes Instrumento MSPI 3 Trimestre 2024 - Ciclo PHVA

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	32%	40%
	Implementación	16%	20%
	Evaluación de desempeño	16%	20%
	Mejora continua	16%	20%
TOTAL		80%	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.

Etapa de Planificación. Durante el desarrollo de la auditoría se evidenció un 32% de avance en esta etapa.

Ilustración 3. Idartes Instrumento MSPI 3 Trimestre 2024 - Etapa de Planificación

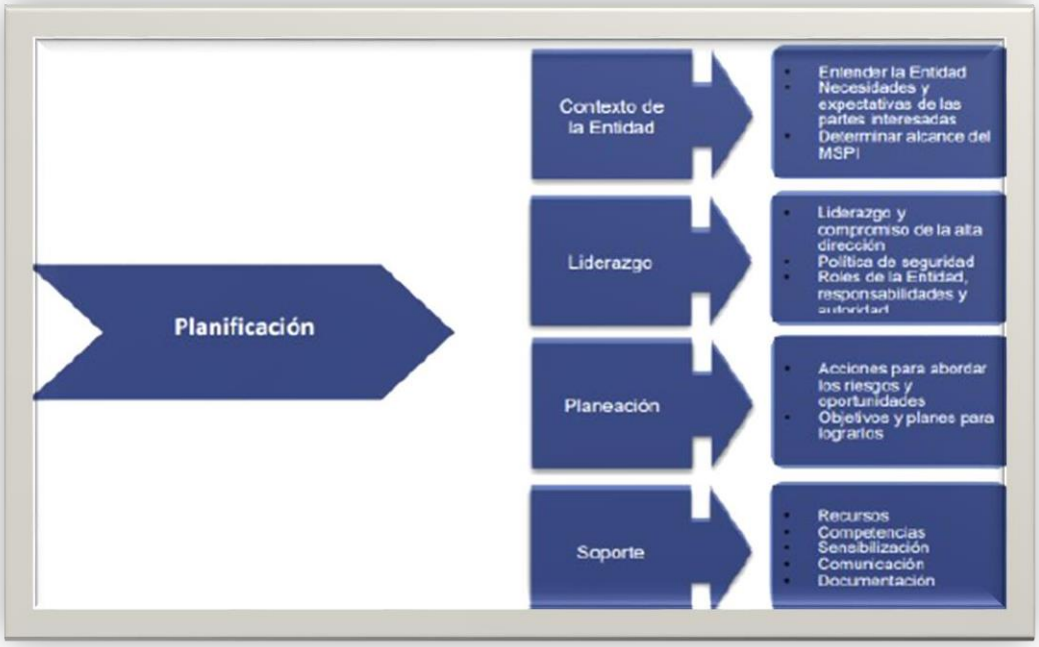
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	32%	40%

[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*

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, v6*), publicado el 2 de febrero de 2024, que algunas de estas actividades no han finalizado, se encuentran en desarrollo y tienen fechas de culminación para diciembre 31 de 2024.

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



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:

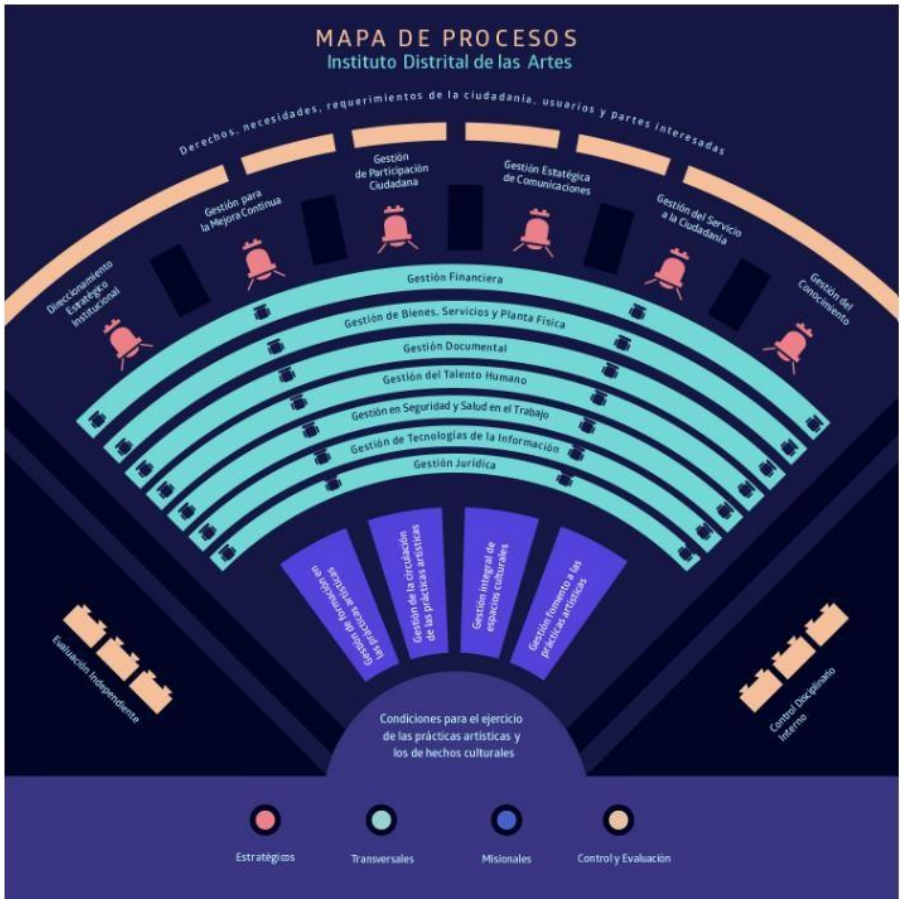
[3] *El contexto de la organización se encuentra desarrollado en la cláusula número 4.0 de la norma ISO/IEC 27001:2013*

[4] *https://comunicarte.idartes.gov.co/SIG/direccionamiento-estrategico-institucional*

- Caracterización Proceso de Direccionamiento Estratégico Institucional (DEI-C-01 v2).
- Caracterización del Proceso de Gestión para la Mejora Continua (GMC-C-01 v4) del 30 de octubre 2023.
- Procedimiento de la Implementación del Modelo Integrado de Planeación y Gestión – MIPG (DIR-PD-11 v2) del 13 de septiembre de 2024.
- Plan Estratégico Institucional (DIR-DSIG-04 v4) octubre 17 de 2024.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (GTI-P-01 v7) febrero 13 de 2024.
- Plan de Continuidad de Tecnologías de la Información (GTI-P-06 v2) septiembre 13 de 2024).
- 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).
- Plan Estratégico de Tecnologías de la Información – PETI (GTI-P-05 v6) febrero 13 de 2024.
- Políticas Digital de Seguridad de la Información (GTI-POL-02 v6) septiembre 24 de 24
- Plan de Seguridad y Privacidad de la Información (GTI-P-02 v6) febrero 2 de 2024.
- Documento Técnico Iniciativas Misionales (DIR-DSIG-03 v1) marzo 27 de 2024.
- Instructivo Consulta Riesgos en Sistema de Información Pandora (GMC-INS-1 v1) febrero 22 de 2024.

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 2025-2029, 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***.

Ilustración 5. Mapa de Procesos del Idartes



Liderazgo y compromiso

El Liderazgo[5] 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 v6)"* 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.

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

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 v6)",* publicado el 24 de septiembre de 2024, 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.

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 76 políticas aprobadas por la Oficina Asesora de Planeación y Tecnologías de la Información:

Tabla 3. Relación de políticas encontradas en el documento GTI-POL-02v6

Ítem	Lineamiento
10.1	Control SGSI-A.6.1 - Organización interna
10.2	Control SGSI-A.6.2.1 - Política para dispositivos móviles
10.3	Control SGSI-A.6.2.2 Política para teletrabajo
10.4	Control SGSI-A.7.1.1 - Selección

Ítem	Lineamiento
10.5	Control SGSI-A.7.1.2 - Términos y condiciones del empleo
10.6	Control SGSI-A.7.2.1 - Responsabilidades de la Dirección
10.7	Control SGSI-A.7.2.2 - Toma de conciencia y formación en la seguridad de la información
10.8	Control SGSI-A.7.2.3 - Proceso disciplinario
10.9	Control SGSI-A.7.3.1 - Terminación o cambio de responsabilidades de empleo
10.10	Control SGSI-A.8.1.1 – A.8.1.2 - Inventario y propiedad de los activos
10.11	Control SGSI-A.8.1.3 - Uso aceptable de los activos
10.12	Control SGSI-A.8.1.4 - Devolución de activos
10.13	Control SGSI-A.8.2.1 - Clasificación de la información
10.14	Control SGSI-A.8.2.2 - A.8.2.3 - Etiquetado de la información manejo de activos
10.15	Control SGSI-A.8.3.1 - Gestión de medios removibles
10.16	Control SGSI-A.8.3.2 - Disposición de los medios
10.17	Control SGSI-A.8.3.3 - Transferencia de medios físicos
10.18	Control SGSI-A.9.1.1 – A.9.1.2 - Política de control de acceso, a redes y a servicios de red
10.19	Control SGSI-A.9.2.1 Registro y cancelación del registro de usuarios
10.20	Control SGSI-A.9.2.2 Suministro de acceso de usuarios
10.21	Control SGSI-A.9.2.3 Gestión de derechos de acceso privilegiado
10.22	Control SGSI-A.9.2.5 Revisión de los derechos de acceso de usuarios
10.23	Control SGSI-A.9.2.6 Retiro o ajuste de los derechos de acceso
10.24	Control SGSI A.9.3.1 – A.9.4.3 - Uso de información secreta para la autenticación y gestión de contraseñas
10.25	Control SGSI-A.9.4.1 Restricción de acceso a la información
10.26	Control SGSI-A.9.4.2 Procedimiento de ingreso seguro
10.27	Control SGSI-A.9.4.4 Uso de programas utilitarios especiales
10.28	Control SGSI-A.9.4.5 Control de acceso a códigos fuente de programas
10.29	Control SGSI-A.10.1.1 – A.10.1.2 - Política sobre el uso de controles criptográficos y gestión de llaves
10.30	Control SGSI-A.11.1.1 Perímetro de seguridad física
10.31	Control SGSI A.11.1.2 – 11.1.3 Controles de acceso físicos Seguridad de oficinas, recintos e instalaciones
10.32	Control SGSI-A.11.1.4 Protección contra amenazas externas y ambientales
10.33	Control SGSI-A.11.1.5 Trabajo en áreas seguras
10.34	Control SGSI-A.11.1.6 Áreas de despacho y carga
10.35	Control SGSI-A.11.2.1 Ubicación y protección de los equipos
10.36	Control SGSI-A.11.2.2 Servicio de suministro
10.37	Control SGSI-A.11.2.3 Seguridad en el Cableado
10.38	Control SGSI-A.11.2.4 Mantenimiento de equipos
10.39	Control SGSI-A.11.2.5 Retiro de activos
10.40	Control SGSI-A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
10.41	Control SGSI-A.11.2.7 Disposición segura o reutilización de equipos

Ítem	Lineamiento
10.42	Control SGSI-A.11.2.8 – A.11.2.9 Equipos de usuarios desatendidos Política de escritorio y pantalla limpia
10.43	Control SGSI-A.12.1.1 Procedimientos de Operación Documentados
10.44	Control SGSI-A.12.1.2 Gestión de cambios
10.45	Control SGSI-A.12.1.3 Gestión de capacidad
10.46	Control SGSI-A.12.1.4 Separación de los ambientes de desarrollo, pruebas y producción
10.47	Control SGSI-A.12.2.1 Controles contra códigos maliciosos
10.48	Control SGSI-A.12.3.1 Respaldo de la información
10.49	Control SGSI-A.12.4 Registro (Logging) y Seguimiento
10.50	Control SGSI-A.12.5 Instalación de software en sistemas operativos
10.51	Control SGSI-A.12.6.1 Gestión de vulnerabilidad técnica
10.52	Control SGSI-A.12.6.2 Restricciones sobre la instalación de Software
10.53	Control SGSI-A.12.7 Consideraciones sobre auditorias de sistemas de información
10.54	Control SGSI A.13.1 Gestión de la Seguridad de las redes
10.55	Control SGSI-A.13.1.1 – SGSI-A.13.1.2 – SGSI-A.13.1.3 Controles de redes Seguridad de servicios de las aplicaciones en redes públicas protección de transacciones de los servicios de las aplicaciones
10.56	Control SGSI-A.13.2.1 -A.13.2 2 Políticas y Procedimientos de Transferencia de información Acuerdos sobre transferencia de información
10.57	Control SGSI-A.13.2.3 Mensajería electrónica
10.58	Control SGSI-A.13.2.4 Acuerdos de confidencialidad o de no divulgación
10.59	Control SGSI-A.14.1.1 Análisis y especificación de requisitos de seguridad de la información
10.60	Control SGSI-A.14.2.1 Política de desarrollo seguro
10.61	Control SGSI-A.14.2.2 - SGSI-A.14.2.3 - SGSI-A.14.2.4 Procedimientos de control de cambios en sistemas - Revisión técnica de las aplicaciones después de cambios en la plataforma de operación - Restricciones en los cambios a los paquetes de software
10.62	Control SGSI-A.14.2.5 – SGSI-A.14.2.6 Principios de construcción de sistemas seguros Ambiente de desarrollo Seguro
10.63	Control SGSI-A.14.2.7 Desarrollo contratado externamente
10.64	Control SGSI-A.14.2.8 – SGSI-A.14.2.9 Pruebas de seguridad de sistemas - Prueba de aceptación de sistemas
10.65	Control SGSI-A.14.3.1 Protección de datos de Prueba
10.66	Control SGSI-A.15 Seguridad de la información para las relaciones con proveedores - Tratamiento de la seguridad dentro de los acuerdos con proveedores - Cadena de suministro de tecnología de información - Seguimiento y revisión de los servicios de los proveedores.
10.67	Control SGSI-A.16.1.1 – A.16.1.7 Responsabilidad y procedimientos - Reporte de eventos de seguridad de la información - Reporte de debilidades de seguridad de la información - Evaluación de eventos de seguridad de la información y decisiones sobre ellos - Respuesta a incidentes de seguridad de la información - Aprendizaje obtenido de los incidentes de seguridad de la información - Recolección de evidencia
10.68	Control SGSI A.17.1.1 Planificación de la continuidad de la seguridad de la información

Ítem	Lineamiento
10.69	Control SGSI-A.17.1.2 Implementación de la continuidad de la seguridad de la información
10.70	Control SGSI-A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
10.71	Control SGSI A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
10.72	Control SGSI-A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
10.73	Control SGSI-A.18.1.2 Derechos de propiedad Intelectual
10.74	Control SGSI A.18.1. 3 - SGSI A.18.1.5 Protección de Registros - Reglamentación de controles criptográficos
10.75	Control SGSI A.18.1.4 Privacidad y protección de información de datos personales
10.76	Control SGSI A.18.2 Revisión independiente de la seguridad de la información - Cumplimiento con las políticas y normas de seguridad - Revisión del cumplimiento técnico

Roles y responsabilidades

El MSPI propuesto por el MinTIC, indica que las "*entidades deben definir internamente las responsabilidades*"[6] 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
- Responsabilidades de los propietarios de la información (funcionarios, contratistas y otros terceros).

[6] *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*

Sin embargo, los numerales "3.2.1.4. Política de seguridad digital de MIPG[7]" y "7.2.3 Roles y responsabilidades[8]" 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[9]":

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.

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[10] 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 v7), del 13 de febrero de 2024, 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) y el Instructivo Consulta de Riesgos en el Sistema de Información PANDORA (GMC-INS-1 v1) febrero 22 de 2024. Así mismo, no se evidenció que Idartes cuente con un 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, sólo un Formato de Activos de Información (GTI-F-23) julio 29 de 2024.

---

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

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

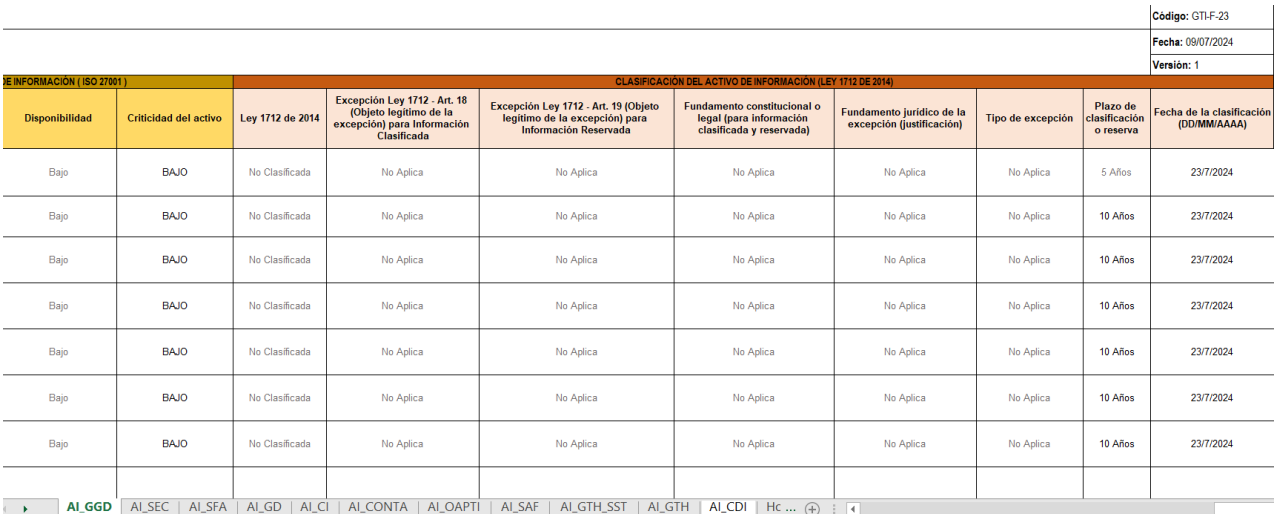
[9] *El MinTIC propone la "Guía 4- Roles y responsabilidades" para desarrollar este ítem, sin embargo, el IDARTES podrá incorporarla o no. Link: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150523_G4_Roles_responsabilidades.pdf*

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

Inventario de Activos de Información en Idartes

Durante la auditoría se evidenció la implementación del formato GTI-F-23 v1 para diligenciar el “Inventario y Clasificación de los Activos de Información” en Idartes, sin embargo, el documento entregado denominado “Registro Activos de Información 2024.xlsx”, contiene un listado de activos de información identificados por 11 procesos – con fecha 9 de julio de 2024 (Activos de Información de GGD, SEC, SFA, GD, CI, CONTA, OAPTI, SAF, GTH,-SST, GTH y CDI). Está pendiente la gestión de diligenciamiento de los 8 procesos faltantes del Idartes.

Ilustración 7. Captura de pantalla Matriz de Activos de Información



Código: GTI-F-23
Fecha: 09/07/2024
Versión: 1

DE INFORMACIÓN (ISO 27001)		CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (LEY 1712 DE 2014)							
Disponibilidad	Criticidad del activo	Ley 1712 de 2014	Excepción Ley 1712 - Art. 18 (Objeto legítimo de la excepción) para Información Clasificada	Excepción Ley 1712 - Art. 19 (Objeto legítimo de la excepción) para Información Reservada	Fundamento constitucional o legal (para información clasificada y reservada)	Fundamento jurídico de la excepción (justificación)	Tipo de excepción	Plazo de clasificación o reserva	Fecha de la clasificación (DD/MM/AAAA)
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	5 Años	23/7/2024
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	10 Años	23/7/2024
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	10 Años	23/7/2024
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	10 Años	23/7/2024
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	10 Años	23/7/2024
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	10 Años	23/7/2024
Bajo	BAJO	No Clasificada	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	10 Años	23/7/2024

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, v6) publicada el 19 de noviembre de 2024, un Procedimiento de Administración de Riesgos (GMC-PD-03, v4) publicado el 2 de octubre de 2024 y un Plan de Tratamiento de Riesgos de Seguridad de la Información (GTI-P-01 v7) publicado el 13 de febrero 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 sistema de información de Pandora el “Mapa de riesgos de Seguridad en la Información 2024” 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 analizan los riesgos de confidencialidad, integridad y

disponibilidad, por activos o grupos de activos del proceso de Gestión de Tecnologías de la Información".

Se evidenció un riesgo de los 10 identificados en el MSPI en el sistema PANDORA: "*Pérdida de integridad, debido a la ausencia o deficiencia en los sistemas de autenticación de los aplicativos y uso inadecuado".*

Ilustración 8. Generación del pdf de un riesgo MSPI

11/12/24, 12:50 planeacionpandorad.idartes.gov.co/sig/riesgo/generarPDFSeguridad

ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE	**Proceso: GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Objetivo Proceso: Gestionar los servicios de tecnologías de la información, a través de estrategias conforme a los lineamientos nacionales y distritales aplicables, promoviendo la implementación de tecnologías de cuarta revolución a la oferta institucional, para alcanzar el uso, apropiación y fortalecimiento de las capacidades tecnológicas desde y hacia los agentes internos y externos, para optimizar el desarrollo de los procesos estratégicos, misionales y de apoyo en cumplimiento de los objetivos institucionales.**	**Código:**	**GTI-C-01**
		Fecha:	**2024-08-20**
	perdida de integridad, debido a la ausencia o deficiencia en los sistemas de autenticación de los aplicativos y uso inadecuado	**Versión:**	**1**
		Página	

1. IDENTIFICACION DEL RIESGO:						
Dependencia: perdida de integridad, debido a la ausencia o deficiencia en los sistemas de autenticación de los aplicativos y uso inadecuado	**Unidad de Gestión o Área**	**Otra**				
Activo: Bases de datos de los sistemas de información.						
Tipo Activo: BASES DE DATOS						
Tipo Riesgo: PERDIDA DE INTEGRIDAD						
Vulnerabilidades: Ausencia o deficiencia en los sistemas de autenticación de los aplicativos. Uso inadecuado en los accesos de autenticación a los sistemas de información.						
Amenazas: No se aplican controles permitiendo el acceso sin credenciales a la información almacenada y procesada en los datos de los sistemas de información. Cambio involuntario de datos en un sistema de información, afectando la operación de la entidad.						
Descripción del riesgo: Posibilidad de afectación reputacional por demandas, investigaciones disciplinarias y/o reclamos por parte de usuarios, por la perdida de integridad, debido a la ausencia o deficiencia en los sistemas de autenticación de los aplicativos y uso inadecuado						
Clasificación del Riesgo: Daños a activos fijos/ eventos externos	**Frecuencia: La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año**	**Detalle Frecuencia: 500**	**Probabilidad inherente: Media 60%**	**Impacto inherente Impacto Reputacional**	**Impacto inherente: Menor 40%**	**Zona de Riesgo inherente Moderado**

Plan de tratamiento de los riesgos de seguridad de la información y declaración de aplicabilidad

Durante el desarrollo de la auditoría se evidenció el procedimiento GTI-P-01 v7 publicado el 13 de febrero de 2024, desarrollado para 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 evidencia 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 del periodo anual 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 v6) publicado en febrero de 2024.

Con respecto al documento denominado “Declaración de Aplicabilidad Anexo A ISO 27001:2013” de Idartes. Durante el desarrollo de la auditoría se evidenció el documento denominado Formato EI-F-02 “Declaración de Aplicabilidad Anexo A ISO 27001:2013” del Instituto, publicado el 3 de noviembre de 2023, y se describe en el título: "*Se emite la presente declaración de aplicabilidad de controles para el Modelo de Seguridad y Privacidad de la Información - MSPI, en función al Comité Directivo del IDARTES y a la Oficina Asesora de Planeación y Tecnologías de la Información, OAP-TI, como responsables de implementar, mantener y mejorar el MSPI a través del Plan de Seguridad y Privacidad de la Información, en ese sentido los controles aplicables para la operación del MSPI, son los numerales que se relacionan a continuación en el campo “CONTROL ISO 27001”, teniendo como base las recomendaciones de la norma NTC/ISO 27001:2013”.*

La declaración de aplicabilidad se aplica anualmente y se tiene definido que será el oficial de seguridad de la información del Idartes el encargado de su aplicación y de socialización de los resultados y las recomendaciones que apliquen.

Ilustración 9. Captura de pantalla Declaración de Aplicabilidad Controles MSPI

	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Código: GTI-F-21
		Fecha: 13/02/2024
	DECLARACIÓN DE APLICABILIDAD DE LA NORMA ISO 27001:2013	Versión: 1
		Página: 1 de 1

Se emite la presente declaración de aplicabilidad de controles para el Modelo de Seguridad y Privacidad de la Información - MSPI, en función al Comité Directivo del IDARTES y a la Oficina Asesora de Planeación y Tecnologías de la Información, OAP-

N°	CONTROL ISO 27001:201	DOMINIO/SUBDOMINIO	CONTROL APLICADO	CONTROLES IMPLEMENTADOS SÍ / NO	EXCLUSIÓN DE CONTROLES SÍ / NO	JUSTIFICACIÓN CONTROLES EXCLUIDO	DECLARACIÓN DE APLICABILIDAD
1	5.	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN					
2	5.1	Orientación de la dirección para la gestión de la seguridad de la información					
3	5.1.1	Políticas para la seguridad de la información	A.5.1.1	SI	NO		Se adopta este control porque es necesario salvaguardar la información en sus pilares de Integridad, confidencialidad y disponibilidad la cual es aprobada por la Oficina de Planeación y Tecnologías de la Información y las Comunicaciones y será divulgada conto dos los empleados (funcionarios, contratistas) y partes externas pertinentes. Políticas de Seguridad de la Información https://comunicarte.idartes.gov.co/sites/default/files/Doc_SIG/Pol%C3%ADtica%20de%20seguridad%20y%20privacidad%20de%20la%20informaci%C3%B3n.pdf
4	5.1.2	Revisión de las políticas de seguridad de la información	A.5.1.2	SI	NO		Se adopta este control porque es necesario verificar periódicamente las Políticas y Normas de Seguridad de la Información, en caso de requerir actualizaciones, modificaciones o adiciones. Idartes, a través de la Oficina de Planeación y Tecnologías de la Información, hará revisión anualmente de las Políticas y Normas de Seguridad de la Información

Soporte de Recursos

Competencia, toma de conciencia y comunicación

El Instituto Distritales de las Artes aún no cuenta con un programa o plan implementado de capacitación de seguridad y privacidad de la información. Se evidenciaron algunos cursos virtuales específicos de varios temas relacionados con la gestión de seguridad y privacidad de la información, y por el canal de Comunicaciones del Instituto[11] se reciben recomendaciones esporádicas 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.

Para este requisito se presenta la estructura de un Programa de Seguridad y Privacidad de la Información del MSPI denominado "Curso de Idartes5",.con tres (3) temáticas de contenido en Políticas de Seguridad de la Información, Activos de Información e Incidentes de seguridad de la información para su implementación periodo 2025.

Ilustración 10. Captura de pantalla Declaración de Aplicabilidad Controles MSPI

Etapa de Operación/Implementación

Durante el desarrollo de la auditoría se evidenció un 16% de avance en esta etapa.

[11] *https://comunicarte.idartes.gov.co/*

Ilustración 11. Idartes Instrumento MSPI 3 Trimestre 2024 - Etapa de Implementación

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Implementación	16%	20%

La etapa de operación[12] 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 12. 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.

[12] *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 v6) fue publicado el 2 de febrero de 2024 y el 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 v6)", 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"[13] propuesto por el MinTIC, la cual se encuentra alineada con los controles definidos en el anexo A de la ISO/EIC 27001:2013.

[13] *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 13. Idartes Instrumento MSPI 3 Trimestre 2024 – Evaluación de Controles Anexo A

No.	Evaluación de Efectividad de controles			Oct. 1° 2024
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	78	100	GESTIONADO
A.9	CONTROL DE ACCESO	80	100	GESTIONADO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	79	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	80	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**78**	**100**	GESTIONADO

La efectividad del control aplicado en el dominio de control A10, 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 A5, A7, A8, A9, A11, A12, A13, A14, A15, A16, A17 y A18 la 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".*

Y para la efectividad del control aplicado en el dominio de control A5, muestra un nivel de efectividad "***Optimizado,*** *las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua".*

A continuación, en la siguiente ilustración se muestra la brecha de los controles Anexo A del MSPI Idartes con corte al 1° de octubre de 2024:

Ilustración 14. Idartes Instrumento MSPI 3 Trimestre 2024 – 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[14]), 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.

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

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 v7)”, publicado el 13 de febrero de 2024, en el que se evidenciaron las actividades que se desarrollarían en la fase de “implementación” del MSPI en el Instituto.

Etapa de Evaluación de desempeño.

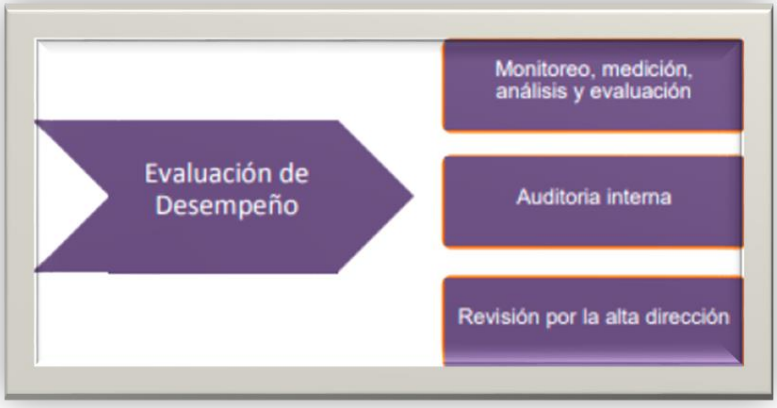
Esta etapa tiene por objetivo la evaluación del desempeño y eficiencia del Modelo de Seguridad y Privacidad de la Información MSPI en el Idartes. Hace parte del “Verificar” en el ciclo PHVA (Planear-Hacer-Verificar- Actuar). Durante el desarrollo de la auditoría se evidenció un avance del 16% en esta etapa:

Ilustración 15. Idartes Instrumento MSPI 3 Trimestre 2024 - Etapa Evaluación de desempeño

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Evaluación de desempeño	16%	20%

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

Ilustración 16. 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 pueda contemplar los lineamientos encontrados en el documento denominado “Guía de Evaluación del Desempeño” u otro similar.

Auditorías internas

La evaluación del MSPI se está haciendo a través de auditorías internas con periodo de frecuencia anual. Durante el desarrollo de la auditoría se evidenció que esta fue la segunda auditoría que se hace al MSPI en el Instituto Distrital de Artes. Por consiguiente, se cuenta con indicadores de evaluación que nos permite medir el avance de las actividades desarrolladas respecto al modelo implementado en el Idartes, así:

Ilustración 17. Comparativo de Evaluación de Controles 2023-2024

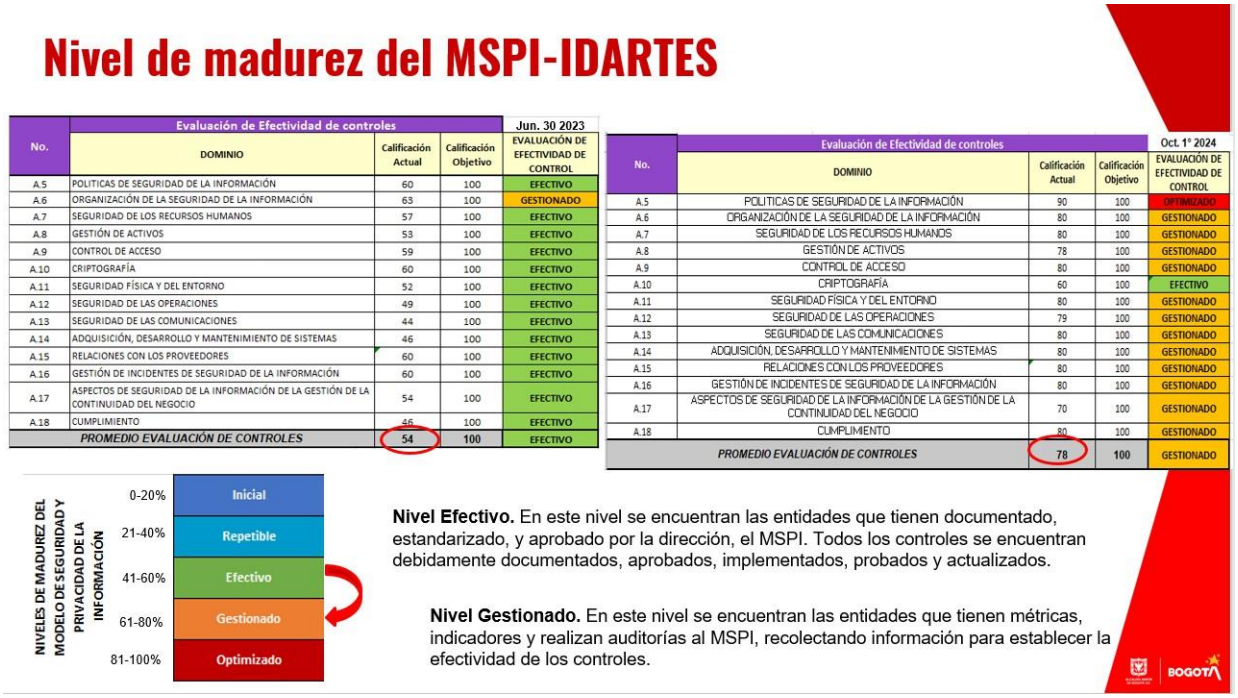
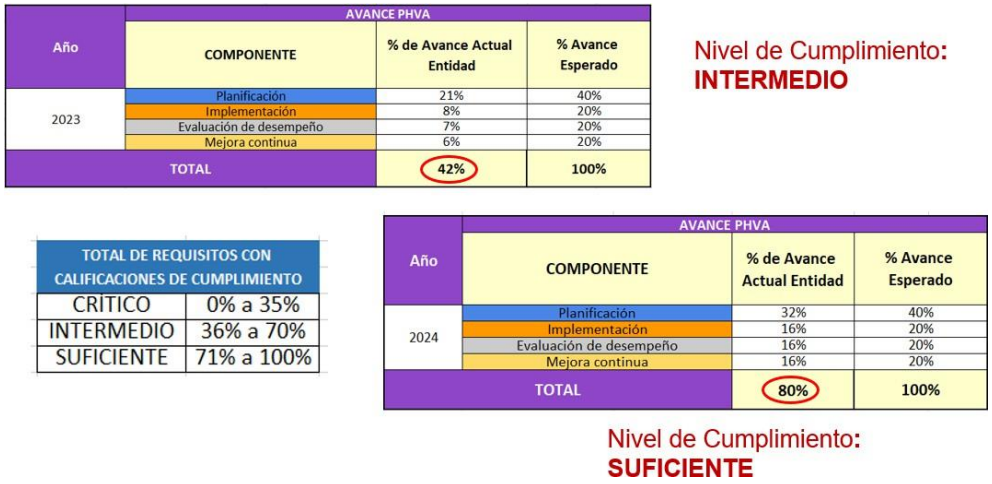


Ilustración 18. Comparativo de Evaluación de Controles 2023-2024



Año	AVANCE PHVA		
	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%

Nivel de Cumplimiento: **INTERMEDIO**

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	32%	40%
	Implementación	16%	20%
	Evaluación de desempeño	16%	20%
	Mejora continua	16%	20%
TOTAL		80%	100%

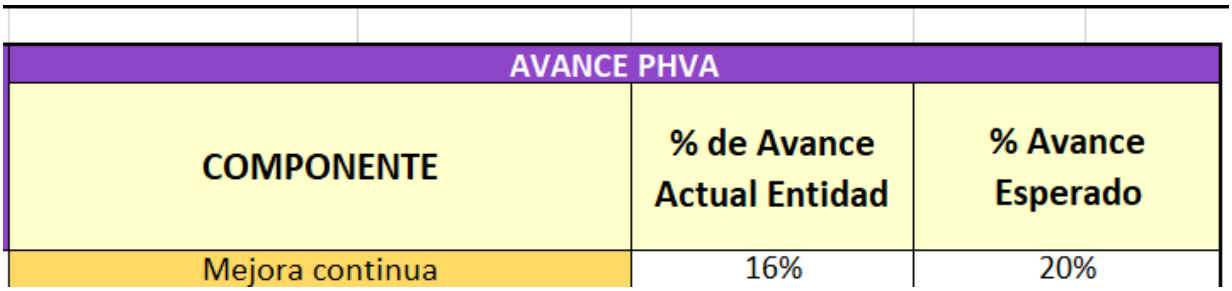
Nivel de Cumplimiento: **SUFICIENTE**

De igual manera, el MSPI que se continue implementando en el Instituto deberá ser revisado[15] y aprobado por la Alta Dirección, cuando así se considere, de tal manera que la Dirección podrá evaluar el avance desde la óptica estratégica.

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 16% en esta etapa:

Ilustración 19. Idartes Instrumento MSPI 3 Trimestre 2024 - Etapa Mejora Continua

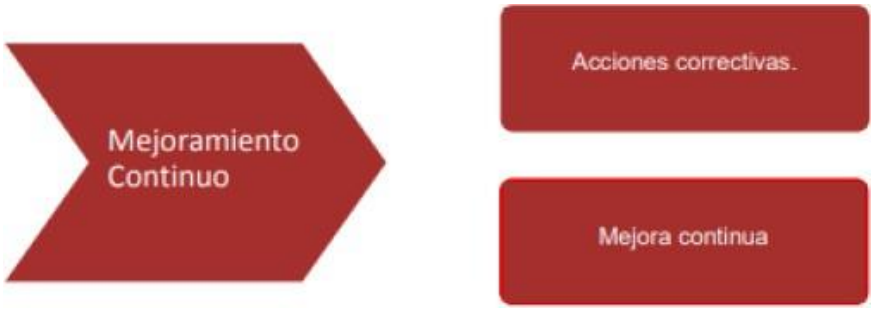


AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Mejora continua	16%	20%

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

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

Ilustración 20. 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.

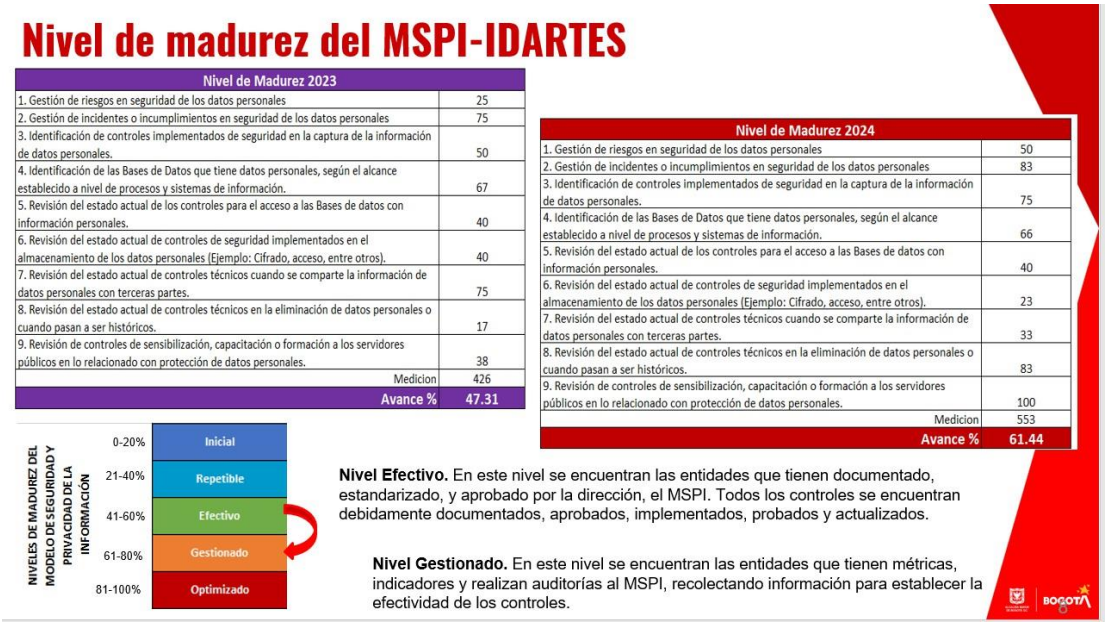
Sin embargo, no se encontraron indicadores, planes de acción o de mejora continua para hacer evaluación o seguimiento al MSPI.

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.

En el mes de julio de 2024 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 21. Matríz de diagnóstico de Protección de Datos Personales – Idartes Ago.2024



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 22. GAP Análisis de la Protección de Datos Personales – Idartes Ago.2024

Por lo anterior se recomienda que esta información de la Gestión de Protección de Datos Personales sea relacionada y forme parte del Instrumento Trasversal del Modelo de Seguridad y Privacidad de la Información MSPI del Idartes, para su pertinente consolidación institucional.

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 25 de noviembre de 2024. 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 2. Diagnóstico MSPI Ciberseguridad 2024

Identificar	Proteger	Detectar	Responder	Recuperar
83%	66%	75%	55%	77%

Ilustración 23. Resultado de dominios Ciberseguridad – Idartes Ago.2024

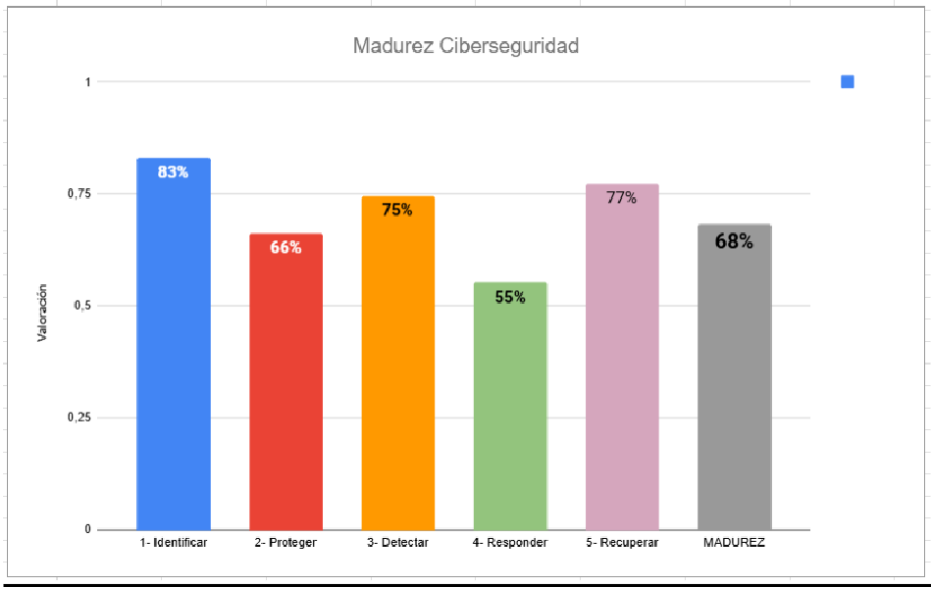


Ilustración 24. Gráfica resultado diagnóstico Ciberseguridad - Idartes Ago.2024

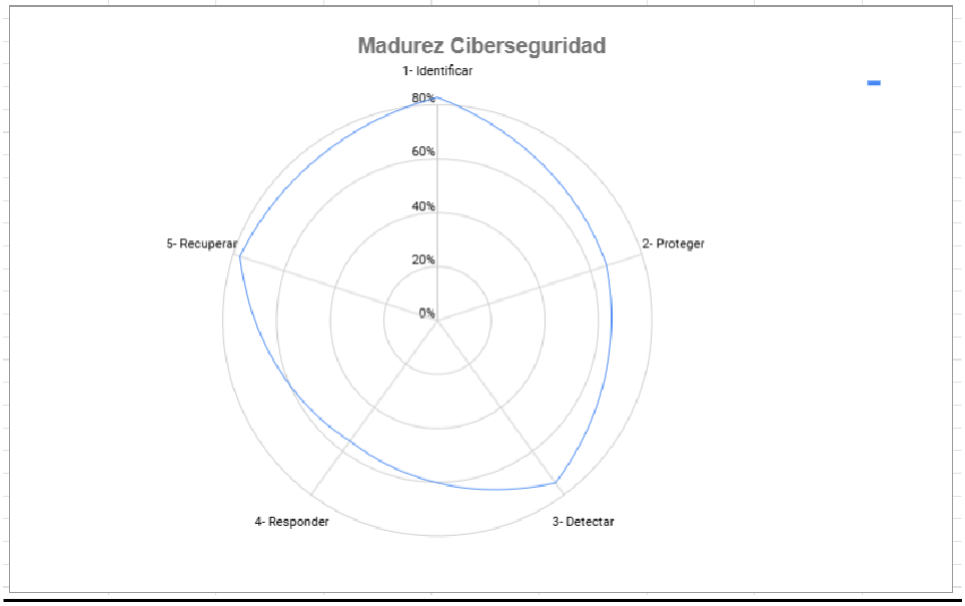
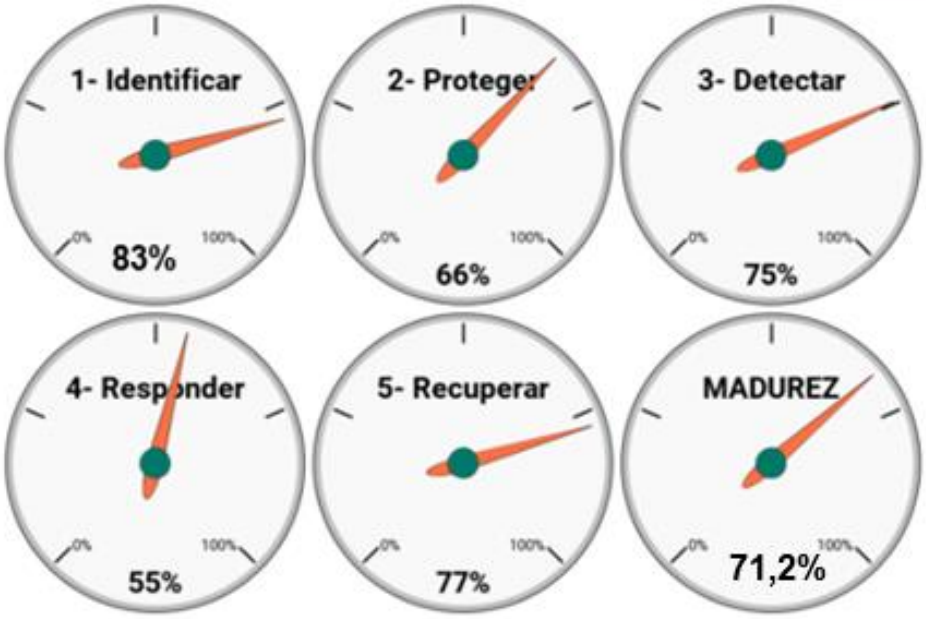


Ilustración 25. Nivel de Madurez por Dominio de Ciberseguridad - Idartes Ago.2024



Por lo anterior se recomienda que esta información de la Gestión de Ciberseguridad sea relacionada y forme parte del Instrumento Trasversal del Modelo de Seguridad y Privacidad de la Información MSPI del Idartes, para su pertinente consolidación institucional.

Resumen de los Resultados de Auditoría

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

Tabla 5. Relación de Resultados de la Auditoría Interna MSPI Procesos

Tipo de Resultado	Cantidad	Referenciación
Fortalezas	3	FO01, FO02, FO03
Cumplimientos	4	CU01, CU02, CU03 y CU04
Observaciones		
Incumplimientos	2	IN01, IN02
Oportunidades de Mejora	7	OM01, OM02, OM03, OM04, OM05, OM06 y OM07.
Total	**16**	

6.1 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. Revisión de Políticas 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).

6.2 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 automatizado 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 y el plan de continuidad del servicio institucional 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.

6.3 OBSERVACIONES

INCUMPLIMIENTOS

IN01. Ajustar el rol del responsable de la seguridad de la información

Se sugiere ajustar el rol y las actividades del responsable de la Seguridad y Privacidad de la Información en el Instituto Distrital de Artes, trasversal a la entidad y cercano a la dirección, de acuerdo con lo propuesto en los numerales “3.2.1.4. Política de seguridad digital” del manual operativo de MIPG y “7.2.3 Roles y responsabilidades” del documento Maestro del Modelo de Seguridad y Privacidad de la Información, que establecen que “se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la alta dirección[16]”.

[16] *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. Octubre 2021*

No se están cumpliendo con las responsabilidades del rol definido en el documento de la Guía del Sistema de Gestión de Seguridad de la Información – SGSI GTI-G-07 del 22 de mayo 2024.

Ilustración 26. Imagen Responsabilidades del Oficial de Seguridad de la Información Idartes

ALCALDÍA MAYOR DE BOGOTÁ D.C.	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	**Código:** GTI-G-07
		Fecha: 22/05/2024
	GUÍA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	**Versión:** 1
		Página: 13 de 17

- Aprobar el Plan de Seguridad y Privacidad de la Información, el Plan de Implementación del Sistema General de Seguridad de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y demás documentación relacionada con el SGSI.

7.2 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información del IDARTES, hace parte de la Oficina Asesora de Planeación y Tecnologías de la Información y es responsable del diseño, desarrollo, implementación, mantenimiento y verificación del correcto funcionamiento del Sistema de Gestión de Seguridad de la Información-SGSI, articulado con los requerimientos normativos vigentes del Ministerio de las TIC y la Alta Consejería Distrital de TIC, el cual tendrá las siguientes responsabilidades:

- Apoyar a las diferentes Unidades de Gestión del IDARTES en el análisis de riesgos de la información.
- Diseñar, desarrollar, establecer y controlar las acciones encaminadas a Seguridad y Privacidad de la Información.
- Establecer los lineamientos, documentación y buenas prácticas de seguridad y privacidad de la información.
- Definir la arquitectura de seguridad de información en línea con la arquitectura de tecnología de la Entidad.
- Determinar e implementar la estrategia de uso y apropiación de seguridad y privacidad de la información.
- Establecer indicadores de gestión de seguridad y privacidad de la información en la Entidad.
- Asesorar en materia de seguridad y privacidad de la información a la Entidad.
- Promover el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en el IDARTES.
- Gestionar los incidentes de seguridad y privacidad de la información reportados e identificados por los funcionarios/contratistas o terceros.

IN02. Implementar una Guía o Instructivo de Registro Propiedad Intelectual

El Instituto no ha realizado el debido registro del software de PANDORA, ante la Dirección Nacional de Derechos de Autor - DNDA, incumpliendo con los requisitos legales establecidos en la Ley 1915 de 2018 (artículo 183). Esto genera un riesgo significativo en términos de protección legal del software como activo de propiedad intelectual, así como posibles vulneraciones a los controles exigidos por la norma ISO/IEC 27001:2013.

Tabla 6. Relación con la Norma ISO/IEC 27001:2013

Dominio/Control	Requerimiento	Impacto del Incumplimiento
A.18.1.1 Cumplimiento	Identificar y cumplir con los requisitos legales aplicables a la seguridad de la información.	La falta de registro implica un incumplimiento legal, exponiendo a la entidad a sanciones administrativas, litigios, pérdida de derechos sobre el software y riesgos reputacionales.
A.8.1 Gestión de Activos	Identificar y gestionar los activos relacionados con la información, incluidas licencias y derechos de autor.	La ausencia de registro demuestra una gestión inadecuada de activos de software, afectando su identificación, propiedad y protección.

Dominio/Control	Requerimiento	Impacto del Incumplimiento
A.15.1.1 Seguridad Partes interesadas	Garantizar que las relaciones con terceros cumplan con los requisitos de seguridad de la información.	Si el software es desarrollado por un proveedor/autor y no se registra, podría haber conflictos legales sobre la titularidad y derechos de uso, incumpliendo con contratos o licencias.

OPORTUNIDADES DE MEJORA

OM01. Alinear los documentos del MSPI con los objetivos estratégicos del Idartes

Se sugiere desarrollar, en la fase de "Planificación", los objetivos, alcance y límites del actual Modelo de Seguridad y Privacidad de la Información MSPI, que se pretende fortalecer la implementación en Idartes, de tal manera que se integren todos 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[17]" propuesto por el MINTIC y lo descrito en la cláusula 1.0 del estándar ISO 27001:2013.

Los objetivos del MSPI deben estar alineados con los objetivos estratégicos, misionales y transversales de Idartes, asegurando su integración en las actividades institucionales.

OM02. Implementar el Plan de capacitación, sensibilización y comunicación MSPI

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 2025, 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 y partes interesadas del Idartes.

OM03. Fortalecer los 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, el Instrumento de evaluación de la Protección de Datos Personales y el Instrumento de evaluación de la Ciberseguridad de Idartes.

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

OM04. 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.

OM05. Articular Instrumento de Gestión Protección de Datos con el MSPI

Se sugiere formalizar el Instrumento de Gestión para la Protección de Datos Personales del Idartes y articularlo con el Modelo de Seguridad y Privacidad de la Información MSPI para fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto.

OM06. Articular Instrumento de Gestión de Ciberseguridad on el MSPI

Se sugiere formalizar el Instrumento de Gestión para la Protección de Datos Personales del Idartes y articularlo con el Modelo de Seguridad y Privacidad de la Información MSPI para fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto.

OM07. Actualización periódica 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.

Teniendo en cuenta lo expuesto en la respuesta al informe preliminar de auditoría interna al MSPI Procesos del Idartes, radicado: 20241200727383 del 19 de diciembre de 2024, se mantiene la observación para establecer las acciones correspondientes en el plan de mejoramiento MSPI 2024.

7. CONCLUSIONES

- Soportados en la documentación del Instrumento MSPI de 2018 a 2024 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 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 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.

8. 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, sistemas de información críticos, servicios institucionales del Instituto Distrital de las Artes – Idartes.

2. Mejorar la gobernanza de la gestión de Seguridad de la Información, incorporando los instrumentos de gestión de la Protección de Datos Personales y la gestión de la Ciberseguridad en el Instrumento o habilitador transversal del Modelo de Seguridad y Privacidad de la Información del Idartes.

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. 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.

5. Formalizar el Instrumento de Gestión para la Protección de Datos Personales del Idartes y articularlo con el MSPI para fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto.

6. Formalizar el Instrumento de Gestión de Ciberseguridad del MSPI para fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior del Instituto.

7. Dar continuidad a la incorporación de los controles formalizados del documento rector del MSPI – Declaración de Aplicabilidad de Controles 2024 – SOA.

Anexo N°.1

DETALLE OBSERVACIONES		
# OBSERVACIÓN	**DESCRIPCIÓN**	**POSIBLE RESPONSABLE**
IN01	Formalizar el rol del responsable de la seguridad de la información	OAPTI
IN02	Implementar una Guía o Instructivo de Registro Propiedad Intelectual	OAPTI
OM1	Alinear los objetivos del MSPI con los objetivos estratégicos, misionales y transversales de Idartes, asegurando su integración en las actividades institucionales.	OAPTI
OM2	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 2025.	OAPTI
OM3	Fortalecer los indicadores del MSPI	OAPTI
OM4	Formalizar procesos, guías e instructivos del MSPI	OAPTI
OM5	Articular el Instrumento de Gestión para la Protección de Datos Personales con el MSPI	OAPTI
OM6	Articular el Instrumento de Gestión de Ciberseguridad con el MSPI	OAPTI
OM7	Actualizar periódicamente el Instrumento MSPI.	OAPTI

Elaboró	Aprobó
CLARA PATRICIA MUÑOZ JIMÉNEZ Contratista de Control Interno	**NÉSTOR FERNANDO AVELLA AVELLA** Asesor de Control Interno