Bogotá D.C, diciembre 18 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 Sistemas de Información Pandora y Orfeo

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 Sistemas de Información Pandora y Orfeo 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 20241300730973 firmado electrónicamente por:

NESTOR FERNANDO AVELLA AVELLA, Asesor Control Interno (e), Área de Control Interno, Fecha firma: 20-12-2024 13:31:27

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

Anexos: 1 folios

eb3189a1447ec2ad4d5698103f5fba97a72f112e81bce898a6dccfe4bd693af8
Codigo de Verificación CV: b219f Comprobar desde:

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

SISTEMAS DE INFORMACIÓN DE PANDORA Y ORFEO

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.

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 de los Sistemas de Información de PANDORA y ORFEO,*** 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 desarrollo y mantenimiento de los Sistemas de Información de PANDORA y ORFEO del Idartes y entrevistas a los auditados de los mismos. Es responsabilidad de cada líder de los sistemas de información 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 practicada.

1. OBJETIVO GENERAL

Evaluar la gestión del Modelo de Seguridad y Privacidad de la información – MSPI en los Sistemas de Información de PANDORA y ORFEO 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

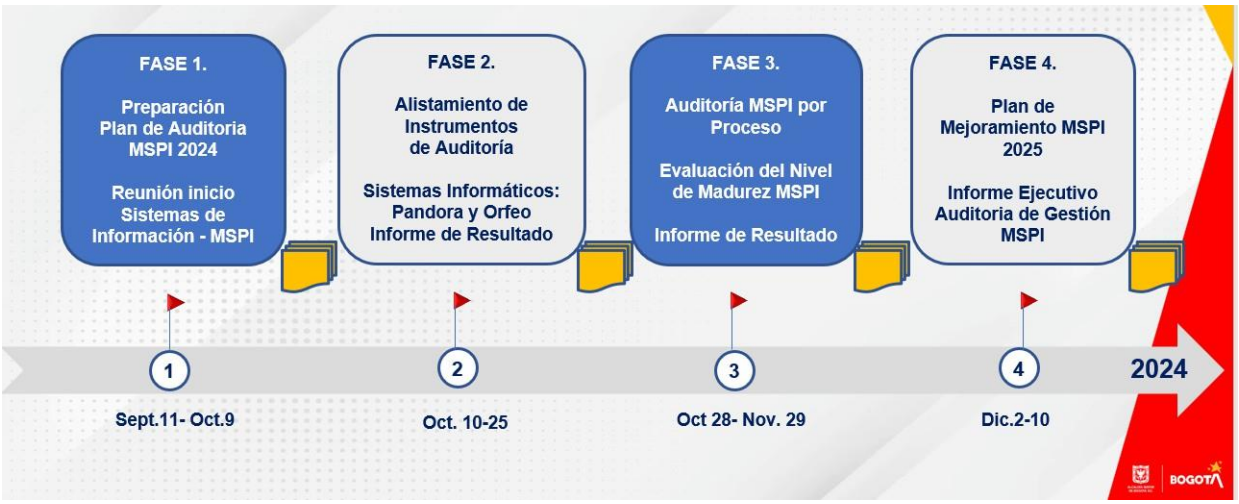
El período a evaluar es el comprendido entre el 01 de enero de 2024 y el 30 de noviembre de 2024, donde se realizó la auditoría interna al Modelo de Seguridad y Privacidad de la Información para Sistemas de Información de PANDORA y ORFEO de Idartes, según los requisitos de la norma ISO/IEC 27001:2013 y los objetivos de control contemplados en la norma ISO/IEC 27002. Período de ejecución de la auditoría interna: Del 15 de octubre al 28 de noviembre de 2024.

Alineación con los Objetivos Estratégicos del Instituto: **“Bogotá Confía en su Gobierno:” OE11:** “Fortalecer la infraestructura tecnológica, comunicativa y la gestión institucional que permitan el fortalecimiento de las capacidades del talento humano con el fin de mejorar la prestación del servicio a la ciudadanía”.

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.

  La evaluación de los sistemas de información se realizó mediante la auditoría interna, teniendo como referente la norma ISO/IEC 27001:2013 y el código de buenas prácticas ISO/IEC 27002 y complementarias, con el fin de determinar el mantenimiento, la mejora continua y la implementación de las iniciativas del MSPI. Se realizará la verificación de la gestión y los componentes de control en lo que tiene que ver con: ambiente de control, actividades de control, gestión del riesgo, actividades de monitoreo e información y comunicación.

4. CRITERIOS DE AUDITORÍA

- 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 Institucional 2020-2024.

- 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.

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.

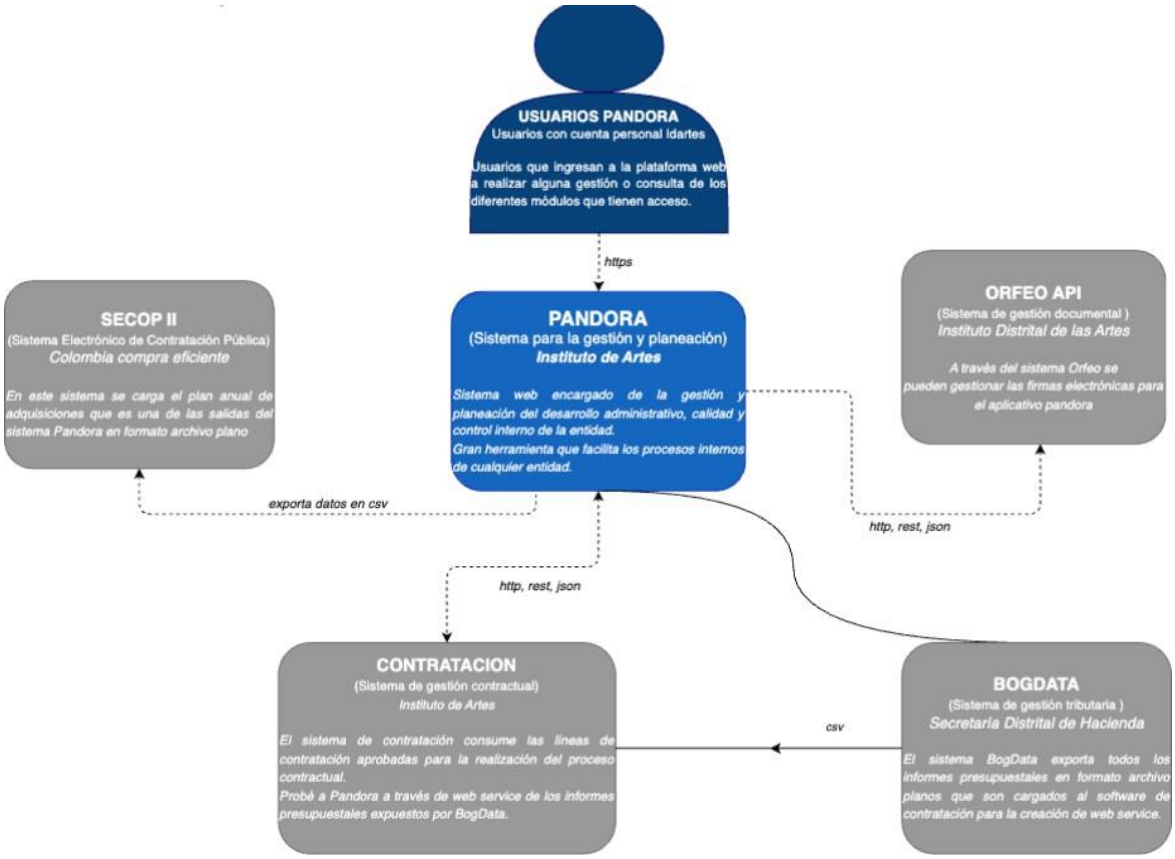
6. RESULTADOS DE LA AUDITORÍA

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 Derechos de Autor del Software PANDORA y ORFEO, 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.

Ilustración 2. Diagrama de Contexto de PANDORA y ORFEO



Fuente: Diagrama Relacional Sistemas de Información TI

Finalmente, 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.

El plan de las sesiones presenciales de auditoría interna de gestión MSPI, se realizó con los líderes de los Sistemas de Información de PANDORA y ORFEO 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.

Tabla 1. Programación de las Sesiones de Auditoría Interna MSPI PANDORA y ORFEO

Id	Sesión Auditoría Interna	Fecha	Criterios Auditoría
SA01	Sistema de Información PANDORA. Gestión de Riesgos, Políticas de Seguridad y Gestión Incidentes	Octubre 15/2024 9 a 11 am	A06 Organización MSPI A05 Políticas MSPI A16 Gestión de Incidentes
SA02	Sistema de Información I PANDORA. Gestión de Continuidad del Servicio y Cumplimiento	Octubre 15/2024 2 a 4 pm	A08 Gestión Activos A12 Continuidad de Servicio A18 Cumplimiento
SA03	Sistema de Información PANDORA. Control de Acceso y Criptografía	Octubre 16/2024 9 a 11 am	A07 Recursos Humanos A09 Control de Acceso A10 Criptografía
SA04	Sistema de Información PANDORA. Seguridad de Operaciones y Adquisición, Desarrollo y Mantenimiento	Octubre 16/2024 2:30 a 4 pm	A11 Seguridad física y entorno A12 Seguridad de Operaciones A14 Adquisición, D/llo y Mant.
SA05	Sistema de Información PANDORA. Seguimiento Plan de Mejoramiento	Octubre 17/2024 9 a 11 am	N09 Evaluación y desempeño N10 Mejora continua
SA06	Sistema de Información PANDORA. Presentación Resultados Auditoría	Octubre 18/2024 9 a 11 am	Lista de chequeo MSPI Pandora. Informe Preliminar.
SA07	Sistema de Información ORFEO. Gestión de Riesgos, Políticas de Seguridad y Gestión Incidentes	Octubre 21/2024 2:30 a 4 pm	A06 Organización MSPI A05 Políticas MSPI A16 Gestión de Incidentes
SA08	Sistema de Información ORFEO. Gestión de Recursos e Información Documental	Octubre 22/2024 9 a 11 am	7.1 Recursos 7.5 Información documentada
SA09	Sistema de Información ORFEO. Seguridad de Operaciones, Gestión de Incidentes y Continuidad de Servicio	Octubre 22/2024 2:30 a 4 pm	A12 Seguridad en la Operaciones A17 Gestión de Continuidad
SA10	Sistema de Información ORFEO. Evaluación del Desempeño y Mejora Continua.	Octubre 23/2024 2:30 a 4 pm	09 Evaluación del Desempeño 10 Mejora .
SA11	Sistema de Información ORFEO. Resultados	Octubre 28/2024 2:30 a 4 pm	Lista de chequeo MSPI Orfeo. Informe Preliminar.
SA15	Gestión de Datos Personales	Nov. 22/2024 2:30 a 4 pm	Lista de chequeo MSPI Cumplimiento Ley de Protección Datos Personales.
SP18	Auditoría Interna Proceso Gestión Jurídica. Aplicación Ley de Propiedad Intelectual para PANDORA y ORFEO.	Nov. 28/2024 11 a 12:30pm	Lista de chequeo MSPI Cumplimiento Ley de Privacidad de la Información.

En el expediente de la auditoría interna MSPI No. 2024100019090000006E se tiene registrado en la plataforma de PANDORA y 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:

Tabla 2. Requisitos de la Norma ISO/IEC 27001:2013

Requerimientos de la Norma ISO/IEC 27001:2013	Cumple	Oportunidad de Mejora	Total general
5. Liderazgo			
5.1 Liderazgo y compromiso	2	1	3
5.2 Política	5		5
5.3 Roles organizacionales, responsabilidades y autoridades	1	1	2
6. Planificación			
6.1 Acciones para atender riesgos y oportunidades	2	1	3
6.2 Objetivos de seguridad de la información y planes para alcanzarlos	1		1
7. Apoyo			
7.1 Recursos	1		1
7.2 Competencias	1		1
7.3 Conciencia	1	1	2
7.4 Comunicación	1		1
7.5 Información documentada	1	1	2
8. Operación			
8.1 Planeación y control operacional	1	2	3
8.2 Evaluación de riesgos en seguridad de la información	1	1	2
8.3 Tratamiento de riesgos en seguridad de la información	1		1
9. Evaluación de Desempeño			
9.1 Supervisión, medición, análisis y evaluación	1	1	2
9.2 Auditoría Interna	1		1
9.3 Revisión por la Dirección	1		1
10. Mejora			
10.1 No conformidades y acciones correctivas	1		1
10.2 Mejora continua	1		1
Total general	24	9	33

La tabla resume la evaluación realizada frente a las 6 cláusulas y 33 requisitos seleccionados, de los cuales 24 es decir el 73% de estos requisitos, están conformes mientras que 9 requisitos es decir 27%, requieren iniciar una oportunidad de mejora. Es importante señalar que, en este último, los requisitos se cumplen, pero es indispensable dar inicio a un plan de mejoramiento para fortalecer y afianzar cada uno de estos elementos.

Tabla 3. Controles de la Norma ISO/IEC 27002

Dominio	Requerimientos de la Norma ISO/IEC 27001:2013	Cumple
A5.	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	
A5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	1
A5.1.2	Revisión de las políticas de seguridad de la información	1
A6.	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades para la seguridad de la información	1
A6.1.5	Seguridad de la información en la gestión de proyectos	
A8.	**GESTIÓN DE ACTIVOS**	
A8.1	**Responsabilidad por los activos**	
A8.1.1	Inventario de activos	1
A8.1.2	Propiedad de los activos	
A8.1.3	Uso aceptable de los activos	1
A8.2	**Clasificación de la información**	
A8.2.1	Clasificación de la información	1
A8.2.2	Etiquetado de la información	
A8.2.3	Manejo de activos	1
A9.	**CONTROL DE ACCESO**	
A9.1	**Requisitos del negocio para control de acceso**	
A9.1.1	Política de control de acceso	1
A9.1.2	Acceso a redes y a servicios en red	
A9.2	**Gestión de acceso a usuarios**	
A9.2.1	Registro y cancelación del registro de usuarios	1
A9.2.2	Suministro de acceso de usuarios	1
A9.2.3	Gestión de derechos de acceso privilegiado	
A9.2.4	Gestión de información de autenticación secreta de usuarios	1
A9.2.5	Revisión de los derechos de acceso de usuarios	
A9.2.6	Retiro o ajuste de los derechos de acceso	
A9.3	**Responsabilidades de los usuarios**	
A9.3.1	Uso de información secreta para la autenticación	1
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción de acceso a la información	1
A9.4.2	Procedimiento de ingreso seguro	
A9.4.3	Sistema de gestión de contraseñas	1
A9.4.4	Uso de programas utilitarios privilegiados	
A9.4.5	Control de acceso a códigos fuente de programas	1

A10.	**CRIPTOGRAFÍA**	
A10.1	**Controles criptográficos**	
A10.1.1	Política sobre el uso de controles criptográficos	1
A10.1.2	Gestión de llaves	1
A12.	**SEGURIDAD DE LAS OPERACIONES**	
A12.1	**Procedimientos operacionales y responsabilidades**	
A12.1.1	Procedimientos de operación documentados	
A12.1.2	Gestión de cambios	1
A12.1.3	Gestión de capacidad	
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	
A12.2	**Protección contra códigos maliciosos**	
A12.2.1	Controles contra códigos maliciosos	1
A12.3	**Copias de respaldo**	
A12.3.1	Respaldo de información	1
A12.4	**Registro y seguimiento**	
A12.4.1	Registro de eventos	1
A12.4.2	Protección de la información de registro	
A12.4.3	Registros del administrador del operador	
A12.4.4	Sincronización de relojes	
A12.5	**Control de software operacional**	
A12.5.1	Instalación de software en sistemas operativos	1
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	1
A12.6.2	Restricciones sobre la instalación de software	
A12.7	**Consideraciones sobre auditorías de sistemas de información**	
A12.7.1	Controles de auditorías de sistemas de información	
A13.2	**Transferencia de información**	
A13.2.1	Políticas y procedimientos de transferencia de información	1
A13.2.2	Acuerdos sobre transferencia de información	1
A13.2.3	Mensajería electrónica	
A13.2.4	Acuerdos de confidencialidad o de no divulgación	1
A14.	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	
A14.1	**Requisitos de seguridad de los sistemas de información**	
A14.1.1	Análisis y especificación de requisitos de seguridad de la información	1
A14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	
A14.1.3	Protección de transacciones de los servicios de las aplicaciones	1
A14.2	**Seguridad en los procesos de desarrollo y de soporte**	
A14.2.1	Política de desarrollo seguro	1
A14.2.2	Procedimientos de control de cambios en sistemas	
A14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	
A14.2.4	Restricciones en los cambios a los paquetes de software	
A14.2.5	Principios de construcción de los sistemas seguros	

A14.2.6	Ambiente de desarrollo seguro	1
A14.2.7	Desarrollo contratado externamente	
A14.2.8	Pruebas de seguridad de sistemas	1
A14.2.9	Prueba de aceptación de sistemas	1
A14.3	**Datos de prueba**	
A14.3.1	Protección de datos de prueba	
A15.	**RELACIONES CON LOS PROVEEDORES**	
A15.1	**Seguridad de la información en las relaciones con los proveedores**	
A15.1.1	Política de seguridad de la información para las relaciones con los proveedores	
A15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	1
A15.1.3	Cadena de suministro de tecnología de información y comunicación	
A15.2	**Gestión de la prestación de servicios de proveedores**	
A15.2.1	Seguimiento y revisión de los servicios de los proveedores	
A15.2.2	Gestión de cambios en los servicios de los proveedores	
A16.	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	
A16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	
A16.1.1	Responsabilidades y procedimientos	
A16.1.2	Reporte de eventos de seguridad de la información	1
A16.1.3	Reporte de debilidades de seguridad de la información	
A16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	
A16.1.5	Respuesta a incidentes de seguridad de la información	1
A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	
A16.1.7	Recolección de evidencia	
A17.	**ASPECTOS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**	
A17.1	**Continuidad de seguridad de la información**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	1
A17.1.2	Implementación de la continuidad de la seguridad de la información	
A17.1.3	Verificación, revisión y evaluación continuidad de la seguridad de la información	
A17.2	**Redundancias**	
A17.2.1	Disponibilidad de instalaciones de procesamiento de información	
A18.	**CUMPLIMIENTO**	
A18.1	**Cumplimiento de requisitos legales y contractuales**	
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	1
A18.1.2	Derechos de propiedad intelectual	1
A18.1.3	Protección de registros	
A18.1.4	Privacidad y protección de información de datos personales	1
A18.1.5	Reglamentación de controles criptográficos	
A18.2	**Revisiones de seguridad de la información**	
A18.2.1	Revisión independiente de la seguridad de la información	
A18.2.2	Cumplimiento con las políticas y normas de seguridad	
A18.2.3	Revisión del cumplimiento técnico	
	Total Controles	39

La tabla resume la evaluación realizada frente a las 14 dominios y 133 controles registrados en la Declaración de Aplicabilidad MSPI del Idartes, formato GTI-F-21 v1 del 13 de febrero de 2024, de los cuales 39 es decir el 29% de estos controles, fueron validados con las entrevistas a los auditados y las evidencias suministradas en cada una de las sesiones de auditoría interna a los Sistemas de Información de PANDORA y ORFEO.

A continuación, se detallan los resultados tanto de los requerimientos del MSPI y los Controles asociados a la Declaración de Aplicabilidad del Idartes:

Tabla 4. Requerimiento 5.1 Liderazgo y Compromiso

DEFINICION DEL REQUERIMIENTO	Resultado de la Evaluación
5.1 Liderazgo y compromiso Literal d) comunicar la importancia de una gestión de Seguridad de la información eficaz y de la conformidad con los requisitos del MSPI	La Dirección General del Idartes, entendiendo la importancia de una adecuada gestión de seguridad y privacidad de la información, desde 30 de julio de 2018 se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad. Para el Instituto Distrital de las Artes – Idartes, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con el objetivo de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, disponibilidad y privacidad de esta, acorde con las necesidades de los diferentes grupos de interés. Evidencia: GTI-P-02 v6 Plan de Seguridad y Privacidad de la Información. En el documento se encuentra el histórico de cambios del 2 de febrero de 2024, versión 6 correspondiente a “Actualización objetivos, definiciones, contenido y actividades a implementar en el 2024”. 1AP-GJU-F-62 v3 Formato Licencia de Uso de Obra del 19 de abril de 2023, en el documento se encuentra los derechos patrimoniales de Obra. Para mejorar el cumplimiento de la Ley 1915 de 2018 en el desarrollo de software de la aplicación PANDORA, algunas oportunidades clave incluyen: Implementación de políticas de Propiedad Intelectual (PI): Definir y documentar una política interna clara sobre la PI que guíe a los desarrolladores y administradores en el uso adecuado de código fuente, bibliotecas y contenidos. Esto incluye el cumplimiento de licencias de software de terceros y el manejo de derechos de Propiedad Intelectual (A.18.1.2). Algunos temas a tener en cuenta en las oportunidades de mejora: 1. **Capacitación en derechos de autor:** Organizar talleres y sesiones informativas para el equipo de desarrollo sobre los derechos de autor y las implicaciones legales de la Ley 1915 de 2018. La capacitación específica sobre cómo utilizar y atribuir contenido correctamente es clave para evitar infracciones. 2. **Control de acceso y autenticidad del código:** Implementar un sistema de control de versiones que registre las contribuciones de cada miembro del equipo, lo que ayuda a proteger los derechos de autor internos y asegurar la autenticidad y originalidad del código en cada etapa del desarrollo.

	3. **Auditorías periódicas de PI**: Realizar auditorías de propiedad intelectual para verificar el cumplimiento continuo con la Ley 1915. Estas auditorías deben incluir una revisión de código y contenido utilizados para identificar cualquier posible infracción y corregirla de inmediato. 4. **Aplicación de licencias abiertas cuando corresponda:** Fomentar el uso de licencias de software abierto compatibles con la ley, como el uso de licencias que permiten modificaciones siempre que se respeten las condiciones de atribución, de esta manera se minimizan riesgos legales. 5. **Integración de herramientas automáticas de escaneo de PI:** Usar herramientas que verifiquen automáticamente el cumplimiento de licencias y detecten posibles problemas de derechos de autor en las bibliotecas de software. Esto permite identificar y gestionar el riesgo de incumplimiento con mayor precisión.

Tabla 5. Requerimiento 5.3 Roles organizacionales, responsabilidades y autoridades

DEFINICION DEL CONTROL	Resultado de la Evaluación
5.3 Roles organizacionales, responsabilidades y autoridades La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados.	Se tiene establecido que la Dirección General debe brindar evidencia de su compromiso con la formulación, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar la información en la Entidad. A través de un Comité Institucional de Gestión y Desempeño del Idartes es la responsable de la aprobación y de realizar el seguimiento a la estrategia de la implementación de la Política Digital, Seguridad y Privacidad de la Información. Se debe comunicar a la entidad 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 del Instituto. El director, subdirectores, gerentes, jefes de oficinas asesoras tiene la responsabilidad de hacer cumplir las normas y políticas de seguridad de la información establecidas por la Dirección General del Instituto Distrital de las Artes – Idartes. La Oficina Asesora de Planeación y Tecnologías de la Información es la responsable de la elaboración y/o modificación y/o actualización y/o eliminación e implementación, monitoreo y seguimiento de la Política Digital, Seguridad y Privacidad de la Información, asegurando los recursos adecuados y promoviendo así una cultura activa de seguridad en el Instituto. Evidencia: GTI-G-07 v1. Guía del Sistema de Gestión de Seguridad de la Información – SGSI, que proporciona directrices fundamentales para el diagnóstico, planificación, implementación, gestión y mejora continua del Sistema de Gestión de Seguridad de la Información. Este documento cuenta con las necesidades y objetivos específicos, los requisitos de seguridad, los procesos que involucran la manipulación de información, así como los responsables y roles dentro del Idartes. Se definen los siguientes roles: • Comité Directivo. Es parte fundamental en la implementación de un SGSI, el seguimiento y su mejora continua; el apoyo del CIGD del Idartes es de suma importancia, ya que repercute directamente en el cumplimiento de la misión de la entidad. • 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.

	• Directores, subdirectores, gerentes, asesores y jefes de oficina. Estos roles deben asegurar que todos los procedimientos de seguridad y privacidad de la información se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información en el Idartes. Actualmente, Idartes no cuenta con el rol de Oficial de Seguridad y Privacidad de la Información que participe activamente dentro de actividades, en los diseños, desarrollos y pruebas de software, como PANDORA y ORFEO, asegurando que estos sistemas cumplan con estándares de seguridad y privacidad. No obstante, de tener un contratista de soporte para gestionar el monitoreo de seguridad perimetral y la gestión de riesgos de seguridad digital de la Unidad de Gestión de Tecnologías de la Información y realizando actividades que se requieran para la alineación de MIPG, PETI y MSPI. En el periodo 2024 se ha tenido una rotación de tres (3) personas contratistas.

Tabla 6. Requerimientos MSPI 6.1 Acciones para atender riesgos y oportunidades

<table>
<tr><th>DEFINICION DEL CONTROL</th><th>Resultado de la Evaluación</th></tr>
<tr><td>6.1 Acciones para atender riesgos y oportunidades</td><td>De acuerdo con el Procedimiento de Administración del Riesgo, documento GMC-PD-03 del 2 de octubre de 2024, aplicar a los Sistemas de Información la identificación y evaluación de riesgos de PANDORA y ORFEO.

Desarrollar y mantener un registro de riesgos que documente los riesgos identificados, su nivel de severidad y los controles existentes. Así mismo, actualizar el registro periódicamente para reflejar cambios en el entorno del Instituto.

Planificación de acciones para aprovechar oportunidades, mejorar la resiliencia e implementar controles que no solo mitiguen riesgos, sino que también mejoren la continuidad operativa. Ejemplo: Implementar soluciones en la nube para mejorar la disponibilidad y escalabilidad.

Ejemplo de acciones específicas:

<table>
<tr><th>Riesgo identificado</th><th>Acción Planificada</th><th>Responsable</th><th>Plazo</th></tr>
<tr><td>Fuga de información confidencial</td><td>Implementar cifrado de datos y autenticación 2FA</td><td>TI</td><td>30 días</td></tr>
<tr><td>Vulnerabilidad en sistemas desactualizados</td><td>Realizar actualizaciones y parches mensuales</td><td>Seguridad TI</td><td>1 mes</td></tr>
<tr><td>Acceso no autorizado a sistemas críticos</td><td>Implementar políticas de control de acceso estricto</td><td>Administradores</td><td>45 días</td></tr>
</table>
</td></tr>
</table>

Tabla 7. Requerimientos MSPI 7.3 Concientización

DEFINICION DEL CONTROL	Resultado de la Evaluación
7.3 Concientización	Idartes debe asegurarse de que las personas que trabajan tanto como funcionarios y prestadores de servicios profesionales son conscientes de la política de seguridad y privacidad de la información, su contribución a la efectividad del MSPI y las implicaciones de no cumplir con los lineamientos establecidos por la alta dirección del Idartes. Esto implica la necesidad de realizar actividades de capacitación y concienciación para todos los niveles del Instituto. Esto garantiza que el personal comprenda su rol en el MSPI del Idartes. Evidencia: En el Plan Institucional de Capacitación 2024, GTH-P-05 v6, se tienen considerado el desarrollo de las temáticas de capacitación en Eje 4: TRANSFORMACIÓN DIGITAL Y CIBERCULTURA, sin embargo, no se encuentra alineado este Plan con el que se tienen en el Modelo de Seguridad y Privacidad de la Información MSPI del Idartes. Fomentar una cultura de seguridad de la información, donde todos los empleados y partes interesadas entiendan su papel y responsabilidades. Algunas iniciativas de implementación: • Programas de capacitación periódicos en seguridad, privacidad y ciberseguridad de la información. • Boletines informativos o campañas internas sobre la importancia del cumplimiento del MSPI • Registros de asistencia y evaluación de la capacitación para garantizar efectividad.

Tabla 8. Requerimientos MSPI 7.5 Información Documentada

DEFINICION DEL CONTROL	Resultado de la Evaluación
7.5 Información Documentada	Es un requisito del MSPI garantizar que los documentos relevantes sean consistentes, accesibles y actualizados, promoviendo la transparencia y eficacia en la gestión de seguridad y privacidad sobre los activos de Información del Idartes. La creación y actualización de los activos de información debe incluir identificación, formato, revisión y aprobación. El MSPI debe garantizar la disponibilidad, confidencialidad e integridad de los documentos, así como evitar el uso no intencionado de versiones obsoletas. Evidencia: El pasado 30 de septiembre se implementó por la Unidad de Gestión Documental el Procedimiento de control de revisión del proceso de envío de información del sistema de gestión de documentos electrónicos, cuyo objetivo es que se permita revisar los datos proporcionadas por la Oficina Asesora de Planeación y Tecnologías de la Información, relacionada con el Sistema de Gestión de documentos electrónicos del Idartes, con el fin de verificar la información y garantizar la integridad y confiabilidad de los mismos por parte del Área de Gestión Documental de la Subdirección Administrativa y Financiera. Así mismo, en la sesión de auditoría interna MSPI al Proceso de Gestión Documental, se evidenció que las TRDs de los Procesos del Idartes no se encontraban disponibles en la Página Web de Instituto - , producto de una actualización del Activo de Información (https://www.idartes.gov.co/es) – No se tenía la visualización de los activos de información en la pestaña de Transparencia y Acceso a la Información Pública.

Tabla 9. Requerimiento 8.2 Valoración de riesgo de la seguridad de la información

DEFINICION DEL CONTROL	Resultado de la Evaluación
8.2 Valoración de riesgo de la seguridad de la información La Entidad debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.	Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad de los activos, Pérdida de Integridad de los activos y Pérdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos del Idartes, por esta razón, se genera el Plan de Tratamiento de Riesgo con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad del Idartes define medidas que serán aplicadas en la vigencia 2024. Evidencia: GTI-P-01 v7 Plan de Tratamiento de Riesgos de Seguridad de la Información. En el documento se encuentra el histórico de cambios del 13 de febrero de 2024, versión 7 correspondiente a "*Actualización de riesgos de seguridad y privacidad de la información*". El análisis de los riesgos es parte de todas las actividades asociadas con el Instituto e incluye la interacción con las partes interesadas, donde se considera los contextos externo e interno del Idartes, incluido el comportamiento humano y los demás factores, ya que está basada en los principios, el marco de referencia y el proceso identificado. Evidencia: informe contiene el monitoreo realizado por la Oficina Asesora de Planeación y Tecnologías de Información OAPTI, como responsable de la segunda línea de defensa, a los riesgos de gestión, seguridad de la información y de corrupción del Instituto Distrital de las Artes - IDARTES, presentando resultados y recomendaciones sobre la gestión institucional de riesgos en el periodo mayo – agosto de 2024.(54 riesgos de gestión, 14 riesgos de corrupción, un riesgo fiscal y 10 riesgos de seguridad de la información). Los riesgos son incorporados ahora en el módulo de riesgos de seguridad de la información, controles y planes de acción a través del sistema de información de PANDORA, esto indica que la visualización y seguimiento ya no se realiza en hojas de cálculo. Enlace del Informe: c.1 - Mapas de riesgos | Idartes. 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: Primera línea. Responsable del proceso de tecnología de la información. Segunda línea. Supervisores contractuales y responsables de acompañamiento de calidad. Tercera línea: Oficina de control interno. Enlace del Relación de Activos 2024. Código: GTI-F-23 9 de Julio 2024 v1: • No.11 Base de Datos PANDORA. B.D de Producción para la toma y almacenado del inventario físico de la entidad, actualmente en estado funcional. Criticidad de Riesgo: ALTO. • No.14.Sistema de información de planeación, gestión y direccionamiento estratégico, Software PANDORA, Criticidad de Riesgo: ALTO. • No.15 Sistema de información de apoyo administrativo, Software ORFEO, Criticidad de Riesgo: ALTO.

Tabla 10. Controles ISO/IEC 27002:2013. A10 Criptografía

Dominio y Control	Resultado de la Evaluación
A.10 Criptografía A.10.1.1 Política sobre el uso de controles criptográficos	En el documento GTI-POL-02 v6 Política Digital, Seguridad y Privacidad de la Información se describe en el numeral 10.29. Control SGSI-A.10.1.1 – A.10.1.2 - Política sobre el uso de controles criptográficos y gestión de llaves, la OAPTI establece los lineamientos para los controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios en los siguientes casos: • Para la información digital o electrónica reservada. • Se debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada como reservada cuente con mecanismos de cifrado de datos. • Se debe desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos. • Se debe utilizar controles criptográficos para la transmisión de información clasificada, fuera del ámbito del Idartes. La OAPTI debe asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por los entes rectores de tecnología. • La OAPTI debe disponer de herramientas que permitan el cifrado de medios de almacenamiento de información. • Realizar un inventario y revisión periódica de llaves criptográficas y certificados digitales actualizado (uso, protección y tiempo de vida). Se verificó el cumplimiento de la política sobre el uso de controles criptográficos en los Sistemas de PANDORA y ORFEO. La entidad cuenta con el documento GTI-POL-02 Política digital seguridad y privacidad de la información el cual tiene implementado: • 10.29. Control SGSI-A.10.1.1 – A.10.1.2 - Política sobre el uso de controles criptográficos y gestión de llaves. Dictar lineamientos para el uso adecuado de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información del Idartes, así mismo implementar el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. • 10.74. Control SGSI A.18.1. 3 - SGSI A.18.1.5 Protección de Registros - Reglamentación de controles criptográficos. Dictar lineamientos para cumplir con la protección de registros contra pérdida, destrucción y falsificación aplicando los requisitos legislativos, reglamentarios, contractuales y del Idartes. El Idartes utiliza la gestión de contraseñas seguras a través de la herramienta Keepass, por el equipo de desarrollo y administrador de infraestructura. Se valida el acceso con autorización mediante mecanismos seguros como el uso de Bearer Token, lo que permite garantizar que sólo usuarios o sistemas autorizados puedan interactuar con los recursos de la entidad. Se detalla la importancia de la autenticación y autorización en el uso de estos servicios para prevenir accesos indebidos y mitigar riesgos relacionados con la exposición de información sensible o crítica. Esto está alineado con los principios de seguridad establecidos en la normativa ISO/IEC 27001, especialmente en lo que se refiere al control de acceso a sistemas y la gestión de identidad.

Tabla 11. Controles ISO/IEC 27002:2013. A12.4 Registro y Seguimiento

Dominio y Control	Resultado de la Evaluación
A.12.4 Registro y Seguimiento A.12.4.1 Registro de eventos A 12.4.2 Protección de la información de registro	La entidad cuenta con el documento GTI-PD-03 v4 del 15 de marzo de 2024. Procedimiento Administración Cuentas de Usuario, cuyo objetivo es administrar y gestionar la autenticación de los usuarios para el acceso a los diferentes sistemas de información y recursos tecnológicos dispuestos para el desarrollo de las funciones y/o actividades de los usuarios. El procedimiento inicia con la solicitud de gestión de usuarios, presentada por el solicitante autorizado de cada unidad de gestión en la mesa de servicios de Tecnologías de la Información. Concluye al atender la solicitud, permitiendo al usuario acceder a diversos sistemas de información y recursos tecnológicos a través del canal previamente establecido para este procedimiento. Se verificó el cumplimiento de la política sobre la administración de cuentas de usuario en los Sistemas de PANDORA y ORFEO. La entidad cuenta con el documento GTI-POL-02 Política digital seguridad y privacidad de la información el cual tiene implementado: Política 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. Dictar lineamientos que permitan asegurar al Idartes un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades. Política 10.47 Control SGSI-A.12.2.1 Controles contra códigos maliciosos Implementar controles de detección, prevención y recuperación, así como sensibilizar a los colaboradores del Idartes para la protección contra códigos maliciosos. Evidencia: El 30 de agosto del 2024 Idartes ITSEC entrega un Informe Técnico mensual de Karpersky, el uso de claves de licencia de Antivirus y un reporte de amenazas. Se tiene un total de 765 licencias adquiridas, 752 licencias en uso y 13 licencias disponibles. En el Informe técnico se hacen las siguientes recomendaciones: • Mantener los agentes de seguridad activados y actualizados. • Activar la seguridad en los equipos que se encuentran deshabilitados. • Se recomienda capacitar a los colaboradores respecto a principios básicos de ciberseguridad, con el fin de evitar los contagios que han sido bloqueados por Kaspersky, esto con el fin de tener un sistema más sano. • Es importante mitigar esta clase de amenazas ya que son potencialmente peligrosas para los sistemas de información. Mantener los sistemas de información actualizados. Es importante realizar un plan de trabajo oportuno para implementar las actividades de mejora continua de este tipo de recomendaciones y realizar seguimiento y monitoreo a los controles efectivos de MSPI.

Tabla 12. Controles ISO/IEC 27002:2013. A12.6 Gestión de la Vulnerabilidad Técnica

Dominio y Control	Resultado de la Evaluación
A.12.6 Gestión de las vulnerabilidades técnicas	El Idartes cuenta con el documento GTI-POL-03 v2 del 21 de diciembre de 2023. Política de Desarrollo de Software, cuyo objetivo es establecer las políticas aplicables a todo el ciclo de vida de desarrollo de software para el Idartes, con el fin de regular y establecer el marco normativo interno frente a la gestión y desarrollo de software alineado al cumplimiento de la política de Gobierno Digital, expresada en el Decreto 1008 del 14 de junio de 2018. En el numeral 5. Seguridad. Se describe que toda aplicación del Idartes tendrá la capacidad de proteger la información y los datos de tal forma que los usuarios y/o sistemas no autorizados no puedan acceder a ellos. Para conceder al sistema los principios de integridad, autenticación y disponibilidad al sistema, se proponen los siguientes métodos: • Antes de realizar el paso a producción, todo proyecto de software debe contar con el visto bueno del oficial de seguridad de la entidad o quien sus veces. • Es requisito para el paso a producción que los productos de software cuenten con un documento de análisis de riesgos cómo lo indica la guía de aseguramiento de aplicaciones. • El oficial de seguridad deberá gestionar las vulnerabilidades en el desarrollo del software, revisando con una frecuencia mensual los logs generados por las aplicaciones o por el servidor de aplicaciones. Validar herramientas que permitan la automatización de este proceso. • Se debe proteger la información sensible como (contraseñas, tokens, firmas digitales) en todos sus estados: tránsito, en reposo y en uso por medio de herramientas y técnicas criptográficas que garanticen la integridad y confidencialidad de la información. En la Política 10.51 Control SGSI-A.12.6.1 Gestión de vulnerabilidad técnica, cuyo objetivo es dictar lineamientos para revisar de manera periódica las vulnerabilidades técnicas de los sistemas de información críticos y misionales. Evidencia: Informe del Resultado de las vulnerabilidades o errores en la configuración a nivel de aplicación del Sistema Pandora – UAECD. Nov. 2023. Se utilizaron un compendio de metodologías entre las cuales se encuentran, PTES (Penetration Testing Execution Standard) y OWASP (Open Web Application Security Project), entre otras. Se realizaron las siguientes recomendaciones: • Las vulnerabilidades con prioridad alta se deben remediar a corto plazo, es decir, se debe solucionar lo que las está produciendo; para las vulnerabilidades medias se deben crear remediaciones sin tanta prioridad. Remediar las vulnerabilidades a las tecnologías de Apache HTTP Server, OpenSSL y OpenSSH. • Hacer uso de metodologías de desarrollo seguro (OWASP, Correctness by Construction [CbyC] o Secure Development Lifecycle [SDL]). Impedir la entrada de código malicioso, escapando los caracteres que son introducidos por los usuarios, es decir, sanitizar las entradas, por ejemplo, bloquear caracteres especiales que no sean letras ni números. Es importante realizar un plan de trabajo oportuno para implementar las actividades de mejora continua de este tipo de recomendaciones y realizar seguimiento y monitoreo a los controles efectivos de MSPI.

Tabla 13. Controles ISO/IEC 27002:2013. A14 Adquisición, desarrollo y mantenimiento del SW-1

Dominio y Control	Resultado de la Evaluación
A.14 Adquisición, desarrollo y mantenimiento del sistema A.14.1.1 Análisis y especificación de requisitos de seguridad de la información A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	El Idartes cuenta con el documento GTI-POL-02 Política digital seguridad y privacidad de la información el cual tiene implementado los siguientes Controles: • Política 10.59. Control SGSI-A.14.1.1 Análisis y especificación de requisitos de seguridad de la información. Dictar lineamientos que permitan incluir requisitos relacionados con seguridad de la información en nuevos sistemas de información y en las mejoras de los existentes. • Política 10.55. Control SGSI-A.13.1.1 – SGSI-A.13.1.2 – SGSI-A.13.1.3. Dictar lineamientos para la protección de la información en las redes y sus instalaciones de procesamiento de información. Controles de redes Seguridad de servicios de las aplicaciones en redes públicas protección de transacciones de los servicios de las aplicaciones. • Política 10.56. Control SGSI-A.13.2.1 - SGSI-A.13.2.2. Dictar lineamientos de seguridad para la información transferida dentro del Idartes con cualquier entidad externa. Así mismo, en el documento GTI-PD-04 v2 Procedimiento de Mantenimiento y Desarrollo de Software, cuyo objetivo es establecer los lineamientos para el desarrollo y mantenimiento de los Sistemas de Información que permitan la mejora continua de las tareas en las diferentes áreas misionales y administrativas del Instituto Distrital de Artes – Idartes. Su alcance está definido desde el inicio con la recepción de la solicitud del desarrollo y/o actualización del Software sugeridas por los usuarios del área respectiva, y culmina con la entrega del producto establecido en las historias de usuario. Es aplicable para desarrollos de productos de software internos y externos en el IDARTES. para modificaciones y nuevos desarrollos. El ciclo de vida de la gestión de mantenimiento y desarrollo en está fase incluye las siguientes actividades: • Enviar las necesidades, requerimientos de desarrollo y/o actualización de Software de las unidades de gestión solicitantes, las cuales se registran en el Formato de solicitud de desarrollo, actualización software Cod. GTIC-F-13 y lo radica a través de la mesa de ayuda GLPI. La solicitud es asignada de acuerdo con el procedimiento de gestión de solicitudes de mesa de ayuda. • Asignar la solicitud a la persona o equipo de sistema de información. Se analiza la solicitud y se genera propuesta. • Revisar si la solicitud de desarrollo es viable desde el punto de vista técnico, de seguridad, presupuestal o legal y emite concepto de viabilidad a través de la mesa de ayuda. • Valida posibles alternativas de solución. Evidencia de Solicitud de requerimientos de desarrollo: GTI-F-13. Formato de Solicitud De Desarrollo, Actualización o Mantenimiento de Software y/o Formularios. 24 de julio de 2024. Se requiere un módulo de Planeación de PANDORA se llame Planes Institucionales.

Tabla 14. Controles ISO/IEC 27002:2013. A14 Adquisición, Desarrollo y Mantenimiento de SW-2

Dominio y Control	Resultado de la Evaluación
A.14 Adquisición, desarrollo y mantenimiento del sistema A.14.2.1 Política de desarrollo seguro A.14.2.2 Procedimientos de control de cambios en sistemas A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación A.14.2.4 Restricciones en los cambios a los paquetes de software A.14.2.5 Principios de construcción de sistemas seguros A.14.2.6 Ambiente de desarrollo seguro A.14.2.7 Desarrollo contratado externamente A.14.2.8 Pruebas de seguridad de sistemas A.14.2.9 Prueba de aceptación de sistemas	El Idartes cuenta con el documento GTI-POL-02 Política digital seguridad y privacidad de la información el cual tiene implementado los siguientes Controles: • Política 10.60. Control SGSI-A.14.2.1 Política de desarrollo seguro Dictar lineamientos que permitan establecer reglas para el desarrollo de sistemas de información dentro del Idartes. • Política 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 de las aplicaciones después de cambios en la plataforma de operación. Dictar lineamientos que permitan establecer procedimientos y revisión de los cambios de las aplicaciones críticas del Idartes y desalentar los cambios en los paquetes de estos. • Política 10.62. Control SGSI-A.14.2.5 – SGSI-A.14.2.6 Principios de construcción de sistemas seguros. Dictar lineamientos que permitan establecer reglas para los principios de desarrollo de sistemas de información seguros dentro del Idartes, igualmente contar con ambientes de desarrollo seguros para todo el ciclo de vida de los sistemas. • Política 10.63. Control SGSI-A.14.2.7 Desarrollo contratado externamente. Dictar lineamientos que permitan establecer reglas para realizar seguimiento a los desarrollos de sistemas de información contratados externamente para funcionamiento dentro del Idartes. • Política 10.64. Control SGSI-A.14.2.8 – SGSI-A.14.2.9 Pruebas de seguridad de sistemas - Prueba de aceptación de sistemas. Dictar lineamientos que permitan establecer pruebas de seguridad y de aceptación de los sistemas del Idartes. • Política 10.65. Control SGSI-A.14.3.1 Protección de datos de Prueba. Dictar lineamientos que permitan establecer reglas para la protección de datos de pruebas de los Sistemas de Información del Idartes. Así mismo, en el documento GTI-PD-04 v2 Procedimiento de Mantenimiento y Desarrollo de Software, cuyo objetivo es establecer los lineamientos para el desarrollo y mantenimiento de los Sistemas de Información que permitan la mejora continua de las tareas en las diferentes áreas misionales y administrativas. El documento entregado de evidencia OAP-TIC- BASES DE DATOS correspondiente al Informe de restauración Base de Datos de Pandora 2024, detalla el proceso técnico que se ejecutó para la recuperación de la base de datos de la aplicación PANDORA en un ambiente de pruebas, con el objetivo de validar las políticas de backup y la consistencia de los archivos de respaldo que se almacenan en la unidad externa, para lo cual se usaron los backup del día 18 de julio del 2024.

Tabla 15. Controles ISO/IEC 27002:2013. A17 Gestión de Continuidad del Servicio - 1

Dominio y Control	Resultado de la Evaluación
A.17 Aspectos de Seguridad de la Información de la Gestión Continuidad Operación Tecnológica A.17.1.1 Planificación de la continuidad de la seguridad de la información	El Idartes cuenta con el documento GTI-POL-02 Política digital seguridad y privacidad de la información el cual tiene implementado los siguientes Controles: Política 10.68. Control SGSI A.17.1.1 Planificación de la continuidad de la seguridad de la información La OAPTI deberá establecer el plan de recuperación de desastres tecnológicos de la Entidad, por medio del cual se continúe brindando el servicio durante una emergencia o desastre, y restaure los servicios críticos de tecnología identificados. Política 10.69. Control SGSI-A.17.1.2 Implementación de la continuidad de la seguridad de la información Esta política pretende establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. Política 10.70. Control SGSI-A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información, verificar que las pruebas realizadas sean consistentes con el alcance y el objetivo del Plan de Continuidad TI y minimicen la interrupción de las operaciones. En el documento GTI-P-06 v2 del 16 de septiembre de 2024. Plan de Continuidad de TI, cuyo objetivo es desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales. La correcta implementación de la gestión de la continuidad de la operación tecnológica, disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, el Instituto estará preparado para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por ese incidente que comprometa los Sistemas de Información PANDORA y ORFEO. Es importante hacer más visible el Plan de Continuidad TI alineado con el MSPI y el PETI, en el que se referencia la estrategia TI y aporta línea de acción en caso de contingencia ante eventos disruptivos, apoyando la ejecución de los proyectos, contemplando actualizaciones, para lograr los objetivos estratégicos engranados al PETI y el MRAE para comprender, analizar, construir y presentar, con el enfoque de estructuración del Modelo de Gestión Estrategia. En el documento GMC-P-02 v2 del 22 de agosto de 2024. Plan de Continuidad de Negocio. En el cambio de versión 2 se incluye un capítulo “análisis de impacto al negocio y valoración del riesgo”. Se ajusta la matriz de responsabilidades y los pasos a seguir para gestionar el Plan BCP. Se incluye también el capítulo de recuperación y restablecimiento, con una Programa de ejercicios. Por último, se referencia en el documento las recomendaciones de la norma ISO 22301:2019 y la Guía para la preparación de las TIC para la continuidad del negocio, del Ministerio de Tecnologías de la Información y las Comunicaciones.

Tabla 16. Controles ISO/IEC 27002:2013. A17 Gestión de Continuidad del Servicio - 2

Dominio y Control	Resultado de la Evaluación
A.17 Aspectos de Seguridad de la Información de la Gestión Continuidad Operación Tecnológica A.17.1.1. Planeación de la continuidad de seguridad de la información	Se trata de implementar medidas de protección y de recuperación ante posibles desastres para minimizar los daños y facilitar el restablecimiento de las operaciones. Los planes de contingencia son parte de los planes de continuidad donde se establecen las respuestas o tratamientos de las incidencias o contingencias. Al consultar el repositorio documental para el proceso Gestión de Mejora Continua, se encontraron los documentos elaborados: 6. Planes: Plan de Continuidad de Negocio del 24 de agosto de 2024 y 9. Otros: GMC-MT-03 v2 Matriz Plan de continuidad de negocio del 2 de diciembre de 2024. Se definen las actividades preventivas y de respuesta, para reaccionar de manera eficiente ante una eventualidad situación que comprometa el desarrollo de las actividades de gestión institucional, la seguridad de la comunidad institucional o la prestación del servicio. El plan de continuidad del negocio está dirigido a la protección de los servicios, infraestructura y sistemas de información, procesos, proyectos y planes de la entidad, por lo que el conocimiento y la ejecución de actividades estará a cargo de los responsables de las líneas estratégicas y operativas. El Plan inicia con el compromiso de la alta dirección y la identificación de roles, hasta la identificación de situaciones de interrupción de actividades de la entidad y la gestión de las respectivas las acciones necesarias para la restauración de servicios. El Idartes a través del presente documento declara el compromiso institucional para brindar a su comunidad institucional y los grupos de interés, las condiciones para que la gestión misional y operativa mantengan su continuidad frente a situaciones adversas que generen interrupción en la prestación del servicio. Por lo anterior, el compromiso está orientado a: • Asegurar que el plan y objetivos de continuidad del negocio estén establecidos y alineados con la dirección estratégica de la organización • Gestionar los recursos necesarios para el adecuado mantenimiento y continuidad del negocio. • Comunicar a los colaboradores de la entidad que se encuentran descritos en la matriz de responsabilidades del capítulo 8, la importancia de su rol frente a la continuidad del negocio. • Promover la mejora continua de la continuidad del negocio. • Comunicar a los colaboradores de la entidad los lineamientos del presente plan de continuidad del negocio. En las sesiones que se programen del Comité Institucional de Gestión y Desempeño, se aprobará y monitoreará el plan de continuidad. Durante la definición de la planificación institucional se definirán y aprobarán los simulacros, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, en articulación con el Plan de Emergencias y Contingencia liderado por el SSST del Idartes, los cuales se harán de manera planificada y concertada con el Comité de emergencias; y de acuerdo con los recursos económicos con los que se cuente en cada vigencia.

El resultado de la ejecución del plan de auditoria se presenta en detalle mediante las listas de verificación. El informe final es la síntesis del ejercicio realizado. Es importante resaltar que la auditoría interna MSPI realizada a los Sistemas de Información, implicó la revisión y evaluación de acuerdo con el cronograma establecido, las evidencias y soportes suministrados fueron validados junto con las matrices de los activos de información pertenecientes a los diferentes procesos del alcance.

SISTEMA DE INFORMACIÓN PANDORA - SIP

A continuación, se presentan los activos de información relacionados con el Sistema de Información de PANDORA en el formato establecido GTI F-23 v1 del 13 de noviembre de 2024:

Tabla 17. Identificación de Activos de Información MSPI de BD-PANDORA

FORMATO ACTIVOS DE INFORMACIÓN PANDORA Base de Datos. Código: GTI-F-23 v1 09/07/2024	
IDENTIFICACIÓN ACTIVOS DE INFORMACIÓN	
Código del activo de información	11-AI-OAPTI
Nombre de Activo	Base de datos PANDORA
Descripción del activos de información	Base de Datos de Producción para la toma y almacenado del inventario físico de la entidad, actualmente en estado funcional.
Tipo de activo de información	Información
Propietario del activo de información	Unidad de Gestión
Custodio del activo de información	OAPTI
Ubicación del activo de información (Ubicación del activo en medio digital y/o electrónico)	Servidor de archivos
Información Publicada/Disponible	Página web y comunicarte
Enlace de publicación (Link)	https://contratacionpandorad.idartes.gov.co/postcontractual/informeInicio
CLASIFICACIÓN DOCUMENTAL	
Serie	BD PANDORA
FECHA DE ACTIVOS	
Fecha de ingreso o actualización del activo en el inventario	13/11/2024
DATOS PERSONALES (LEY 1581 DE 2012)	
¿Contiene datos personales?	Si
Tipos de datos personales	Datos Semiprivados
CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)	
Confidencialidad	Pública Reservada / Confidencial =Alta
Integridad	Alto
Disponibilidad	Alto
Criticidad del activo	ALTO
CLASIFICACIÓN DE ACTIVOS DE INFORMACION (LEY 1712 DE 2014)	
Ley 1712 de 2014	Información Pública Reservada
Fundamento constitucional o legal (para información clasificada y reservada)	Artículo 15 constitución Política. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar

Tabla 18. Identificación de Activos de Información MSPI de SI-PANDORA

FORMATO ACTIVOS DE INFORMACIÓN PANDORA 2 Sistema de Información. Código: GTI-F-23 v1 09/07/2024	
IDENTIFICACIÓN ACTIVOS DE INFORMACIÓN	
Código del activo de información	15-AI-OAPTI
Nombre de Activo	PANDORA
Descripción del activos de información	Sistemas de información de planeación, gestión y direccionamiento estratégico
Tipo de activo de información	Información
Propietario del activo de información	Unidad de Gestión
Custodio del activo de información	OAPTI
Ubicación del activo de información (Ubicación del activo en medio digital y/o electrónico)	Servidor de archivos
Información Publicada/Disponible	Página web y comunicarte
Enlace de publicación (Link)	https://contratacionpandorad.idartes.gov.co/postcontractual/informe/inicio
CLASIFICACIÓN DOCUMENTAL	
Serie	Sistema de Información PANDORA
FECHA DE ACTIVOS	
Fecha de ingreso o actualización del activo en el inventario	13/11/2024
DATOS PERSONALES (LEY 1581 DE 2012)	
¿Contiene datos personales?	Si
Tipos de datos personales	Datos Semiprivados
CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)	
Confidencialidad	Clasificada / Uso Interno = Medio
Integridad	Alto
Disponibilidad	Alto
Criticidad del activo	**ALTO**
CLASIFICACIÓN DE ACTIVOS DE INFORMACION (LEY 1712 DE 2014)	
Ley 1712 de 2014	Información Pública Clasificada
Fundamento constitucional o legal (para información clasificada y reservada)	No aplica

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

Tabla 19. Relación de Resultados de la Auditoría Interna PANDORA

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	3	OM01, OM02, OM03
Total	**12**	

SIP FORTALEZAS

FO01. **Liderazgo y compromiso**

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

FO02. Gobernanza 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 todas las partes interesadas. (Requerimiento norma 5.2).

La Política Digital, Seguridad y Privacidad de la Información se encuentra en el documento GTI-POL-02 v6, del 24 de septiembre de 2024, cuyo objetivo es "*Establecer lineamientos necesarios, con el fin de fortalecer la gestión de seguridad y privacidad de la Información del Idartes, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información-SGSI, basado en la identificación, valoración y gestión de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio".* Esta actualización abarca la protección de los sistemas de información, redes, aplicaciones, dispositivos y demás activos digitales utilizados en la Entidad.

El Idartes cuenta con el documento GTI-POL-03 v2 del 21 de diciembre de 2023. Política de Desarrollo de Software, cuyo objetivo es "*Establecer las políticas aplicables a todo el ciclo de vida de desarrollo de software para el Idartes, con el fin de regular y establecer el marco normativo interno frente a la gestión y desarrollo de software alineado al cumplimiento de la política de Gobierno Digital, expresada en el Decreto 1008 del 14 de junio de 2018".*

Al contar con estas políticas debidamente documentadas se establecerán los lineamientos que guiarán el comportamiento personal y profesional sobre la información y la construcción de software que el Instituto Distrital de las Artes en su misión de garantizar el ejercicio de los derechos culturales de los habitantes del Distrito Capital gestiona día a día.

FO03. Enfoque integral en la gestión de riesgos de seguridad de la información

La entidad define y aplica la metodología institucional para la gestión de riesgo de seguridad de la información que involucra el Sistema de Información de PANDORA y se evalúa las potenciales consecuencias, determinando los niveles de riesgos, para priorizar actividades en los planes definidos. (Requerimiento norma 6.1.2).

El Idartes cuenta con el documento GMC-PD-03 v4 Procedimiento Administración del Riesgo, cuyo objetivo es *"Identificar, analizar y dar tratamiento a los riesgos de gestión, corrupción y seguridad de la información a los que se encuentre expuesto el Instituto Distrital de las Artes Idartes, y que puedan afectar o impedir el logro de los objetivos estratégicos, para el cumplimiento de su misión institucional. Inicia con la formulación de la Política de Administración del riesgo, la identificación del contexto interno, externo y de proceso para la identificación de los riesgos y termina con el informe de monitoreo de riesgos reportado a la primera y tercera línea de defensa".*

La nueva versión 4 del 2 de octubre del 2024 incluye ajustes en el Módulo de Riesgos de PANDORA, como los actores que desarrollan las actividades de la gestión de riesgos en los Procesos del Idartes, Módulo de Notificaciones PANDORA, actividades relacionadas con materialización de riesgo proveniente de PQRS y la divulgación del informe de monitoreo a los miembros del Comité Directivo del Idartes.

SIP CUMPLIMIENTOS

CU01. Política de Desarrollo de Software alineada con la Política del MSPI

En la planeación del MSPI, 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 Información de PANDORA. (Requerimiento norma 6.1.1).

Las políticas definidas en el documento GTI-POL-03 v2 del 23 de diciembre de 2023, aplican a los servidores públicos, contratistas y practicantes que tienen un vínculo laboral y/o contractual con el Instituto o personal de otras entidades que intervengan en los procesos de desarrollo de software de la entidad, y por tanto tienen acceso a los sistemas de información para el cumplimento de sus labores, obligaciones y funciones, por lo cual, tienen la responsabilidad de velar por los pilares de la seguridad de la información, especialmente si la información se encuentra tipificada como información pública clasificada o pública reservada.

El Idartes cuenta con el Procedimiento Administración Cuentas de Usuario GTI-PD-03 v4, del 29 de diciembre de 2023, cuyo objetivo es "Administrar y gestionar la autenticación de los usuarios para el acceso a los diferentes sistemas de información y recursos tecnológicos dispuestos para el desarrollo de las funciones y/o actividades de los usuarios". El procedimiento inicia con la solicitud de gestión de usuarios, presentada por el solicitante autorizado de cada unidad de gestión en la mesa de servicios de Tecnologías de la Información y concluye al atender la solicitud, permitiendo al usuario acceder a diversos sistemas de información y recursos tecnológicos a través del canal previamente establecido para este procedimiento.

La nueva versión 4 del 15 de marzo de 2024 incluye la actualización de políticas de ajuste en tiempos de vencimiento de usuario de red por la ocasión de la implementación de PANDORA al SSO.

CU02. Cumplimiento del Programa de Capacitación Funcionalidad de Pandora

El control se realiza por medio de las capacitaciones o charlas a los usuarios referentes de los sistemas de información PANDORA y ORFEO del Idartes, así mismo se cuenta con piezas comunicativas de diferentes temas relacionados con la gestión de seguridad y privacidad de la información de la información y contenidos de los módulos con las funcionalidades de los Sistemas de Información de PANDORA Y ORFEO, y se difunde por medio del correo institucional, el cual es remitido de manera masiva a todos los colaboradores del Idartes. (Requerimiento norma 7.1.2).

El pasado 1° de octubre se desarrolló una capacitación de diligenciamiento Informes de pago – Pandora, por la Oficina Asesora de Planeación y Tecnologías de la Información, modalidad virtual HANGOUST MEET y las temáticas a desarrollar fueron: 1. Ingreso a Pandora, 2. Diligenciamiento del Informe de Pago – Gestión, 3. Proceso de firma del informe y 4. Solicitudes de soporte.

El 7 de mayo de 2024, se enviaron piezas de comunicación a la página de Comunicarte del Idartes, los avances en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI y en ciberseguridad por la Oficina de Planeación y Tecnologías de la Información.

Se realizó el 12 de diciembre de 2024 una encuesta de conocimiento y satisfacción de los Servicios de TI en aspectos de seguridad y privacidad de la información, cuyo objetivo era conocer la percepción y el nivel de apropiación de los usuarios internos de las Unidades de Gestión frente a los servicios de TI prestados por la Oficina Asesora de Planeación y Tecnologías de la Información, con el fin de continuar mejorando los servicios y la gestión oportuna de los mismos.

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).

En el documento GTI-P-01 v7 del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, del 13 de febrero de 2024, cuyo objeto es definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información y de Seguridad Digital que el Idartes pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Así mismo, su alcance es de realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información y de Seguridad Digital, que permita integrar en los Sistemas de Información y los procesos del Instituto, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Alineado a una gestión de tratamiento de riesgos de Seguridad y Privacidad de la Información, donde se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Idartes.

CU04. Gestión de vulnerabilidades en el Sistema de Información de Pandora

En el Informe del Resultado de las vulnerabilidades o errores en la configuración a nivel de aplicación del Sistema Pandora – UAECD. Nov. 2023. Se utilizó un compendio de metodologías entre las cuales se encuentran, PTES (Penetration Testing Execution Standard) y OWASP (Open Web Application Security Project), entre otras. Se realizaron las siguientes recomendaciones:

Las vulnerabilidades con prioridad alta se deben remediar a corto plazo, es decir, se debe solucionar lo que las está produciendo; para las vulnerabilidades medias se deben crear remediaciones sin tanta prioridad. Remediar las vulnerabilidades a las tecnologías de Apache HTTP Server, OpenSSL y OpenSSH. Hacer uso de metodologías de desarrollo seguro (OWASP, Correctness by Construction [CbyC] o Secure Development Lifecycle [SDL]). Impedir la entrada de código malicioso, escapando los caracteres que son introducidos por los usuarios, es decir, sanitizar las entradas, por ejemplo, bloquear caracteres especiales que no sean letras ni números. Es importante realizar un plan de trabajo oportuno para implementar las actividades de mejora continua de este tipo de recomendaciones y realizar seguimiento y monitoreo a los controles efectivos de MSPI.

SIP INCUMPLIMIENTO

IN01. 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 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[1]".

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 3. 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.

[1] *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*

IN02. Implementar una Guía o Instructivo de Registro Propiedad Intelectual

La entidad pública Instituto de las Artes Idartes 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 20. 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.
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.

SIP OPORTUNIDADES DE MEJORA

OM01. Integrar mecanismos de seguridad en las fases de desarrollo de PANDORA

Se sugiere desarrollar una oportunidad de mejora para integrar los mecanismos de seguridad en las fases de desarrollo del sistema de información PANDORA, se centra en fortalecer el enfoque de "Seguridad desde el diseño" (Security by Design). Esto implica incluir prácticas de seguridad en todas las etapas del ciclo de vida del desarrollo del sistema, desde la planificación inicial hasta el mantenimiento. A continuación, se describe cómo puede aprovecharse esta oportunidad:

- Planificación y análisis de requisitos. Incorporar requisitos de seguridad desde la definición de las funcionalidades del sistema, asegurando que las necesidades de confidencialidad, integridad, disponibilidad y cumplimiento normativo (como la Ley 1915 de 2018) estén contempladas desde el inicio.

- Diseño del sistema de información. Realizar un diseño orientado a minimizar vulnerabilidades, como la inclusión de modelos de control de acceso, cifrado de datos en tránsito y reposo, y segmentación de componentes críticos.
- Desarrollo. Adoptar prácticas de codificación segura y realizar revisiones de código de manera regular para identificar y corregir vulnerabilidades.
- Pruebas e implementación. Incorporar pruebas de seguridad en las alidaciones funcionales, como pruebas de penetración (pentesting) y análisis dinámico de seguridad (DAST).
- Despliegue y operación. Implementar monitoreo continuo de seguridad, actualizaciones regulares de software y una política de gestión de vulnerabilidades.
- Mantenimiento y mejora continua. Integrar auditorías periódicas de seguridad para evaluar la efectividad de los controles implementados y proponer mejoras.

Integrar estos mecanismos de seguridad no solo aumenta la protección de los datos y la confiabilidad del sistema, sino que también garantiza el cumplimiento normativo, reduce los costos asociados con incidentes de seguridad y mejora la percepción de confianza de los usuarios. Adicionalmente, posicionar a PANDORA como un sistema robusto, capaz de enfrentar los riesgos digitales actuales.

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 2024, 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 del Idartes.

OM03. Implementar un Procedimiento, Guía o Instructivo - Registro Derechos de Autor

Desarrollar un procedimiento, guía o instructivo para realizar el registro de las soluciones de software del Instituto Distrital de las Artes, por intermedio de la página web de la Dirección Nacional de Derechos de Autor - DNDA, alineado con el Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información del Idartes.

La implementación de soluciones y sistemas de información desde las entidades del estado es complementada con el registro de propiedad intelectual, acorde con el Marco de Referencia de Arquitectura Empresarial - MRAE, en el documento maestro del Modelo de Gestión y de Gobierno de TI, en los lineamientos asociados a Sistemas de Información.

La dirección nacional de derechos de autor define un procedimiento de registro presencial basado en formatos, y con base en formatos y documentación impresa y/o en soportes digitales, y un registro en línea disponible desde la página de la DNDA.

El registro de derechos de autor es un paso fundamental para la formalización de la publicación de un sistema de información en la entidad, y se relaciona con la valoración del activo de información, aseguramiento y responsabilidades respecto a su gestión, y formalización de la propiedad del DNP del producto de software.

http://www.registroenlinea.gov.co/portal.htm

El portal habilita el registro de productos de software, con base en documentos soporte exigidos en formatos pdf, y mediante un procedimiento paso a paso.

SISTEMA DE INFORMACIÓN ORFEO – SIO

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

Tabla 21. Relación de Resultados de la Auditoría Interna ORFEO

Tipo de Resultado	Cantidad	Referenciación
Fortalezas	2	FO01, FO02
Cumplimientos	4	CU01, CU02, CU03 y CU04
Observaciones		
Incumplimientos	1	IN01
Oportunidades de Mejora	3	OM01, OM02, OM03
Total	**11**	

Tabla 22. Identificación de Activos de Información MSPI de ORFEO

FORMATO ACTIVOS DE INFORMACIÓN ORFEOSistema de Información. Código: GTI-F-23 v1 09/07/2024	
IDENTIFICACIÓN ACTIVOS DE INFORMACIÓN	
Código del activo de información	14-AI-OAPTI
Nombre de Activo	ORFEO
Descripción del activos de información	Sistemas de información de apoyo administrativo ORFEO
Tipo de activo de información	Información
Propietario del activo de información	Unidad de Gestión
Custodio del activo de información	OAPTI
Ubicación del activo de información (Ubicación del activo en medio digital y/o electrónico)	Servidor de archivos
Información Publicada/Disponible	Página web y comunicarte
Enlace de publicación (Link)	https://contratacionpandorad.idartes.gov.co/postcontractual/informe/inicio
CLASIFICACIÓN DOCUMENTAL	
Serie	Sistema de Información ORFEO
FECHA DE ACTIVOS	
Fecha de ingreso o actualización del activo en el inventario	13/11/2024
DATOS PERSONALES (LEY 1581 DE 2012)	
¿Contiene datos personales?	Si
Tipos de datos personales	Datos Semiprivados
CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)	
Confidencialidad	Clasificada / Uso Interno = Medio
Integridad	Alto
Disponibilidad	Alto
Criticidad del activo	**ALTO**
CLASIFICACIÓN DE ACTIVOS DE INFORMACION (LEY 1712 DE 2014)	
Ley 1712 de 2014	Información Pública Clasificada
Fundamento constitucional o legal (para información clasificada y reservada)	Artículo 15 constitución Política. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar

FORTALEZAS

FO01. Liderazgo y compromiso

La alta dirección demuestra liderazgo y compromiso con respecto al Modelo de Seguridad y Privacidad de la Información – MSPI del Sistema de Información de ORFEO, 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 todas las partes interesadas. (Requerimiento de norma 5.2).

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 todas las partes interesadas. (Requerimiento de norma 5.2).

La Política Digital, Seguridad y Privacidad de la Información se encuentra en el documento GTI-POL-02 v6, del 24 de septiembre de 2024, cuyo objetivo es "*Establecer lineamientos necesarios, con el fin de fortalecer la gestión de seguridad y privacidad de la Información del Idartes, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información-SGSI, basado en la identificación, valoración y gestión de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio".* Esta actualización abarca la protección de los sistemas de información, redes, aplicaciones, dispositivos y demás activos digitales utilizados en la Entidad.

El Idartes cuenta con el documento GTI-POL-03 v2 del 21 de diciembre de 2023. Política de Desarrollo de Software, cuyo objetivo es "*Establecer las políticas aplicables a todo el ciclo de vida de desarrollo de software para el Idartes, con el fin de regular y establecer el marco normativo interno frente a la gestión y desarrollo de software alineado al cumplimiento de la política de Gobierno Digital, expresada en el Decreto 1008 del 14 de junio de 2018".*

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.

SIP INCUMPLIMIENTO

IN01. 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 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[2]”.

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.

[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. Octubre 2021*

Ilustración 3. Imagen Responsabilidades del Oficial de Seguridad de la Información Idartes

- 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.

OPORTUNIDADES DE MEJORA

OM01. Planificación

La oportunidad de mejora para gestionar los riesgos del sistema de información ORFEO y garantizar una interoperabilidad segura entre sistemas internos y externos radica en establecer un marco integral de gestión de riesgos tecnológicos y de interoperabilidad. Este enfoque permite identificar, evaluar, tratar y monitorear los riesgos asociados con el funcionamiento de ORFEO y su interacción con otras plataformas (ver la ilustración 2). A continuación, se detalla esta oportunidad:

- Identificación y análisis de riesgos. Realizar un análisis de riesgos específico para ORFEO, considerando tanto vulnerabilidades internas como amenazas externas que afecten su operación y la interoperabilidad.
- Fortalecimiento de la seguridad en la interoperabilidad. Implementar estándares de seguridad para la interoperabilidad de sistemas, como el uso de APIs seguras, certificados digitales y protocolos de cifrado en la comunicación.
- Monitoreo continuo de los puntos de integración. Mejora: Establecer un monitoreo en tiempo real de las interacciones entre ORFEO y otros sistemas para identificar actividades anómalas o intentos de explotación de vulnerabilidades.
- Políticas y procedimientos claros para la interoperabilidad. Desarrollar políticas para gestionar los riesgos asociados a la interoperabilidad, incluyendo controles de acceso, auditorías y medidas de respuesta ante incidentes.

- Pruebas de seguridad y simulaciones. Realizar pruebas periódicas de seguridad para evaluar la resiliencia de ORFEO y los sistemas interoperables frente a posibles riesgos.
- Capacitación del personal. Capacitar al equipo encargado de ORFEO y las integraciones en buenas prácticas de gestión de riesgos y seguridad de la información.
- Automatización en la gestión de riesgos. Adoptar herramientas de automatización para identificar riesgos, mitigar vulnerabilidades y gestionar incidentes en ORFEO y los sistemas interoperables.

La implementación de estas acciones asegura que ORFEO opere con menores riesgos, fomenta la confianza en los sistemas interoperables, y protege la información crítica manejada por el sistema. Además, una gestión efectiva de riesgos mejora la continuidad operativa, reduce costos relacionados con incidentes y facilita el cumplimiento de regulaciones sobre seguridad de la información y protección de datos.

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 2024, 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 del Idartes.

OM03. 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 Idartes, 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 MSPI, 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[3]”.

[3] *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*

Teniendo en cuenta lo expuesto en la respuesta al informe preliminar de auditoría interna al MSPI Sistemas de Información Pandora y Orfeo, radicado: 20241200721043 del 17 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 y los Sistemas de Información PANDORA y ORFEO que éste ha mostrado avances graduales en términos de conformidad con la norma ISO/IEC 27001. Sin embargo, se requiere definir requisitos de seguridad en los Sistemas de Información, monitorear que la seguridad se diseñe e implemente dentro del ciclo de desarrollo de software, asegurar la protección de los datos mientras se realizan las pruebas y realizar pruebas de funcionalidad de la seguridad y privacidad de la información.
- Se observa una mejora en la gestión y control de la seguridad de la información de estos sistemas de información PANDORA y ORFEO, aunque siguen existiendo funcionalidades 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. Es importante tener un control efectivo en los cambios de versión de licencias y especial cuidado en la depuración de la base de datos migrada de un ambiente de desarrollo al de producción.
- Finalmente, a pesar de los avances observados, el Instituto necesita seguir haciendo esfuerzos considerables para continuar fortaleciendo el MSPI en los Sistemas de Seguridad de la Información de PANDORA y ORFEO 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 de estos Sistemas de Información.

8. RECOMENDACIONES

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

- 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 cercano a la dirección.

- 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 del Idartes.

- Probar el Plan de Continuidad TI, estableciendo los objetivos de los escenarios y 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 los Sistemas de Información, 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.

Anexo N°.1

DETALLE OBSERVACIONES		
# OBSERVACIÓN	**DESCRIPCIÓN**	**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	Integrar mecanismos de seguridad en las fases de desarrollo de PANDORA.	OAPTI
OM2	Plan de capacitación, sensibilización y comunicación	OAPTI
OM3	Integrar mecanismos de seguridad en las fases de desarrollo de ORFEO.	OAPTI
OM4	Gestionar riesgos y plan de tratamiento de riesgos en el Sistema de Información ORFEO	OAPTI

Elaboró	Aprobó
Clara Patricia Muñoz Jiménez Contratista Control Interno	**Néstor Fernando Avella Avella** Asesor de Control Interno