

Oficina Asesora de Planeación y
Tecnologías de la Información.



Informe avance primer
semestre del Plan de
Seguridad y Privacidad de
la Información

2024

Tabla de Contenido

1.	Presentación	3
2.	Objetivo	3
3.	Alcance.....	3
4.	Ficha Técnica.....	4
5.	Herramientas Utilizadas.....	4
6.	Resultado del Monitoreo	4
7.	Avance de Gestión del Primer Semestre 2024.....	6
8.	Conclusiones de Avance de los Planes.....	7
9.	Recomendaciones.....	8
10.	Acciones de mejora para alcanzar el 100% en la implementación de las acciones formuladas del Plan de Seguridad y Privacidad de la Información	8

1. Presentación

La información en las Entidades es considerada hoy en día uno de sus activos más importantes y valiosos, es de vital importancia para la toma de decisiones, para que las Entidades sean más competitivas, innovadoras, presten mejores bienes, servicios y ofrezcan información confiable, ágil y acertada a sus clientes y usuarios. Sin dejar de mencionar que hoy por hoy los Activos de Información, son atacados constantemente, generando un aumento en el número de incidentes de seguridad de la información que generan a las Entidades pérdida de su buena imagen, problemas con sus clientes, pérdidas económicas y problemas legales.

Es por la importancia de la información, que el Instituto Distrital de las Artes – Idartes, a través del documento Plan de Seguridad y Privacidad de la Información establece la planificación, implementación, evaluación y mejora del Modelo de Seguridad y Privacidad de la Información-MSPI, determinado por las necesidades, objetivos, estructura organizacional, los procesos o de la Entidad, así como requisitos legales y exigencias de seguridad de la información dadas por el Ministerio de las TIC establecido en el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 en el artículo 2.2.9.1.1.3 Principios, que define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 que define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital; así como la Resolución 00500 de 2021 y sus anexos que incorporan lineamientos en materia de Seguridad Digital en las entidades del estado.

2. Objetivo

Garantizar la continuidad de las operaciones del Idartes, protegiendo y preservando la confidencialidad, integridad, disponibilidad y privacidad de la información.

3. Alcance

Establecer, implementar y mantener el Modelo de Seguridad y Privacidad de la Información -MSPI, alineado con las normas ISO27001:2013 e ISO 27032, así mismo, con los lineamientos incorporados con la Resolución 00500 de 2021, fortaleciendo la gestión de la Política de Seguridad Digital y Continuidad de la Operación para implementar dentro del Instituto Distrital de las Artes – Idartes.

4. Ficha Técnica

La fuente de información y metodología de seguimiento para el presente informe se compone de:

- Formulación, actualización y divulgación de temas específicos referentes a Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.
- Continuar con la implementación del Modelo de Seguridad y Privacidad de la Información del Idartes.
- Salvaguardar la información producida y procesada por las unidades de gestión del Idartes.
- Administrar, controlar y gestionar los incidentes de la seguridad de la información.
- Optimización de sistemas de apoyo a la infraestructura tecnológica del Idartes.

5. Herramientas Utilizadas

Para realizar el seguimiento del primer semestre al avance de los productos establecidos en el marco de los proyectos formulados en el plan de seguridad y privacidad de la información, se utiliza el correo electrónico, a través de una comunicación por parte de la OAP-TI a cada uno de los responsables por cada uno de los proyectos para la remisión por el mismo medio, de una breve descripción del avance junto con las evidencias que dan cuenta de lo informado, adicionalmente, se cuenta con un instrumento en Excel, el cual permite realizar el autocontrol, seguimiento y mejora de las acciones planeadas en el marco del Plan.

6. Resultado del Monitoreo

En las siguientes tablas se consolida los resultados del monitoreo de avance de las actividades formuladas en el plan de seguridad y privacidad de la información de la vigencia actual.

Resultados del seguimiento y monitoreo del Plan de Seguridad y Privacidad de la Información

ACTIVIDAD	META	PRODUCTO	% AVANCE ACUMULADO	PLAZO DE CUMPLIMIENTO
1. Implementar estrategias de uso y apropiación relacionadas con aspectos de seguridad y privacidad de la información a toda la comunidad del Idartes.	3 Estrategias (correos, charlas, capacitaciones, entre otras) de socialización interna de las Políticas de Seguridad.	3 Estrategias de socialización de Seguridad y Privacidad de la Información.	66%	31/12/2024
2. Actualizar el inventario de activos de información con la clasificación de seguridad y privacidad de la información.	1 documento actualizado con el inventario de activos de información.	1 documento actualizado con el inventario de activos de información.	66%	31/12/2024
3. Restringir el acceso a los códigos fuente de los programas.	1 documento del control implementado de restricción del acceso a códigos fuentes.	1 documento del control de restricción del acceso a códigos fuentes.	33%	31/12/2024
4. Actualizar la documentación de los Planes de recuperación de desastres de TI y el plan de continuidad de TI.	2 documentos actualizados del plan de recuperación de desastres y plan de continuidad de TI.	2 documentos actualizados del plan de recuperación de desastres y plan de continuidad de TI.	66%	31/12/2024

Tabla 1. Resultado del seguimiento y monitoreo Plan de Seguridad y Privacidad de la Información

Resultados del seguimiento y monitoreo Plan de Seguridad y Privacidad de la Información

ACTIVIDAD	META	PRODUCTO	% AVANCE ACUMULADO	PLAZO DE CUMPLIMIENTO
5. Implementar controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	1 Documento con los controles a implementar para las transferencias de información.	1 Documento con los controles a implementar para las transferencias de información.	33%	31/12/2024
6. Asegurar los equipos desatendidos de los usuarios con políticas de protección.	1 documento de informe con el listado de equipos asegurados.	1 documento de informe con el listado de equipos asegurados.	66%	31/12/2024
7. Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	1 documento de registros de administración de los sistemas de información	1 documento de registros de administración de los sistemas de información	33%	31/12/2024
8. Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	1 documento de actualización de administración de infraestructura	1 documento de actualización de administración de infraestructura	66%	31/12/2024

Tabla 2. Resultado del seguimiento y monitoreo Plan de Seguridad y Privacidad de la Información

Resultados del seguimiento y monitoreo del Plan de Seguridad y Privacidad de la Información				
ACTIVIDAD	META	PRODUCTO	% AVANCE ACUMULADO	PLAZO DE CUMPLIMIENTO
9. Elaborar y formalizar un formato para la gestión de cambios, con el cual se controlen los cambios que se efectúen en los sistemas de información, antes del paso a producción de los mismos.	1 formato para la gestión de cambios de sistemas de información	1 formato para la gestión de cambios de sistemas de información	66%	31/12/2024
10. Actualizar el procedimiento de Mantenimiento y Desarrollo de Software donde se incluyan actividades relacionadas con el acuerdo 002 de 2023.	1 documento actualizado de mantenimiento y desarrollo de software	1 documento actualizado de mantenimiento y desarrollo de software	33%	31/12/2024
11. Revisar y actualizar procedimiento Incidentes de Seguridad de la Información.	1 documento actualizado y oficializado de gestión de incidentes de seguridad de la información	1 documento actualizado y oficializado de gestión de incidentes de seguridad de la información	66%	31/12/2024

Tabla 3. Resultado del seguimiento y monitoreo Plan de Seguridad y Privacidad de la Información

7. Avance de Gestión del Primer Semestre 2024

- Capacitaciones y difusiones masivas en temas del uso adecuado de los recursos tecnológicos (Google drive, activos de información, Ciberseguridad, entre otros).
- Formulación y actualización de documentos de seguridad de la información (Política de seguridad de la información, guía gestión de incidentes de seguridad, matriz de riesgos de seguridad de la información, matriz de activos de información, manual del SGSI, plan de continuidad de tecnologías de la información, entre otros).
- Implementación de controles técnicos en los sistemas de seguridad perimetral para el aseguramiento de la plataforma tecnológica.
- Participación en mesas de trabajo con la Alta Consejería Distrital de TIC, en el marco de Gobierno Digital, Seguridad Digital y Ciberseguridad.
- Se realiza un informe de la consola 215 licencias de antivirus donde se puede evidenciar:
 - Informe del uso de claves de licencias, observaciones recomendaciones

- Informe de amenazas, observaciones y recomendaciones
 - Informe uso de base de datos, observaciones y recomendaciones
 - Estado de la protección observaciones y recomendaciones
 - Informe sobre vulnerabilidades Observaciones
 - Conclusiones generales
- Se realiza un informe de seguimiento y monitoreo al FIREWALL:
En las Políticas de Seguridad de la información, actualmente en IDARTES existen 108 Políticas de navegación creadas, el cual de estas 108 se tienen fuera de uso 26 políticas que no están recibiendo ningún tipo de tráfico y no se están utilizando

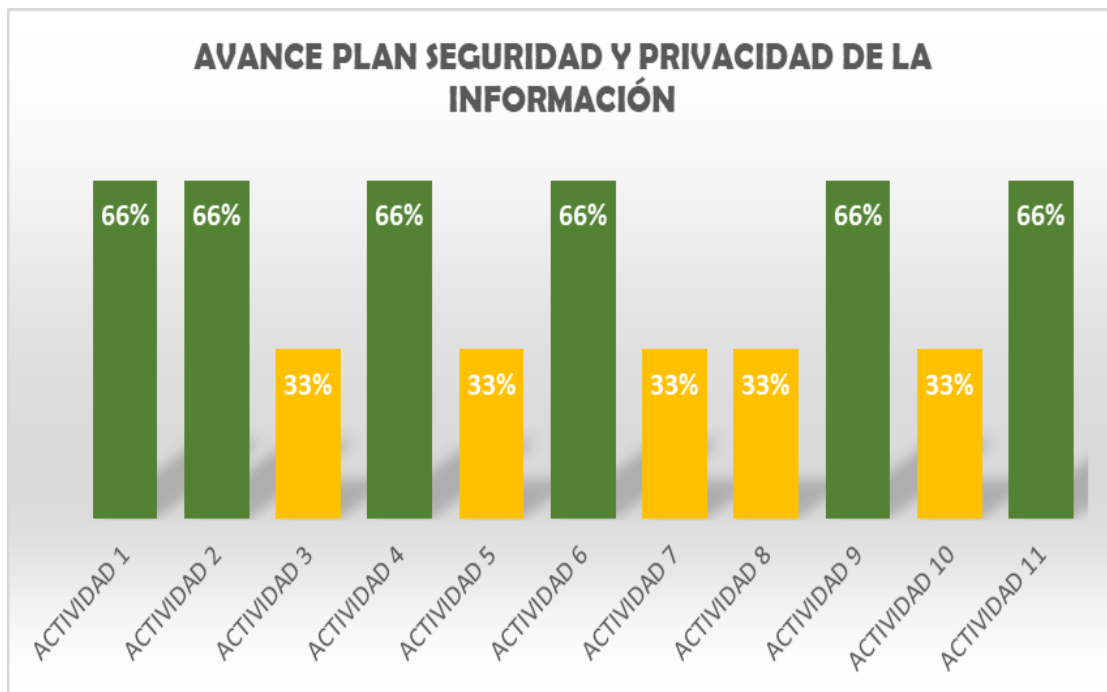


Ilustración 1. Avance del plan de seguridad y privacidad de la información

8. Conclusiones de Avance de los Planes

En este informe se evidencia el seguimiento y monitoreo continuo de las estrategias definidas en el Plan de Seguridad y Privacidad de la Información Durante el desarrollo de estas actividades, se garantiza la ejecución y el seguimiento de cada acción, fortaleciendo los servicios de TI y asegurando la confidencialidad, integridad y disponibilidad de la información en los procesos de la entidad.

La fuente de información y metodología de ejecución para el seguimiento y monitoreo se basa en los siguientes elementos:

- Formulación e implementación de controles a través de la Política de Seguridad y Privacidad de la Información del Idartes.
- Seguimientos y monitoreos cuatrimestrales realizados por la segunda línea de defensa.
- Gestión y tratamiento metódico, documentado y eficiente de los riesgos de seguridad de la información.
- Aplicación de controles, lineamientos y normativas nacionales y distritales de cumplimiento obligatorio para las entidades públicas relacionadas con Gobierno Digital y Seguridad Digital.
- Planificación e implementación de acciones que mejoren los controles ISO27001:2013 de seguridad y privacidad de la información dentro de los flujos de información y servicios de TI.

9. Recomendaciones

Se realiza la revisión y monitoreo constantemente a los lineamientos de buenas prácticas en seguridad de la información para la entidad, alineado al Modelo de Seguridad y Privacidad de la información (MSPI), con la finalidad de fortalecer el aseguramiento de los servicios TI, seguridad de la información y preservar la confidencialidad, integridad y disponibilidad y propender por la continuidad de la operación y servicios de las unidades de gestión del Idartes.

10. Acciones de mejora para alcanzar el 100% en la implementación de las acciones formuladas del Plan de Seguridad y Privacidad de la Información

- Realizar un seguimiento continuo a la ejecución de las acciones que presentan retrasos, con el fin de garantizar su cumplimiento.
- Mejora e implementación de los Controles Técnicos e indicadores de gestión del MSPI:
 - **Actualización de documentos:** Revisar y actualizar la documentación de para reflejar los cambios en el entorno y en el SGSI.
 - **Actualización de sistemas:** Mantener actualizados los sistemas operativos, aplicaciones y software de seguridad.
 - **Fortalecimiento de las redes:** Implementar medidas de seguridad en la red, como firewalls, sistemas de detección de intrusiones y encriptación.

- **Gestión de vulnerabilidades:** Realizar evaluaciones de vulnerabilidades de forma regular y aplicar los parches correspondientes.

Al implementar estas acciones de manera integral y sostenida, se puede avanzar significativamente hacia el objetivo de alcanzar el 100% de implementación del Plan de Seguridad y Privacidad de la Información.

Aprobó: Daniel Sánchez Rojas – Jefe OAP-TI
Elaboró: Martha Mateus – Contratista OAP-TI



Radicado: **20244300566543**

Fecha **08-10-2024 16:42**

Documento 20244300566543 firmado electrónicamente por:

DANIEL SÁNCHEZ ROJAS, Jefe Oficina Asesora de Planeación y Tecnologías de la Información,
Oficina Asesora de Planeación, Fecha de Firma: 08-10-2024 17:01:08

Proyectó: SANDRA PATRICIA MORENO BOHORQUEZ - Técnico Administrativo - Área de Tecnología



a5fa160f1efb89ee4fca0d6eb0b07aebc70b15cdabd0e1ec9332099d942b4034

