



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
CULTURA, RECREACIÓN Y DEPORTE  
Instituto Distrital de las Artes

## **Informe avance primer cuatrimestre del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**

**Oficina Asesora de Planeación y Tecnologías de la Información**

29/05/2025

## TABLA DE CONTENIDO

1.	INTRODUCCIÓN	2
2.	OBJETIVO	3
3.	ALCANCE	3
4.	RESPONSABLES	3
5.	RESULTADOS DEL MONITOREO I CUATRIMESTRE	3
5.1	Implementación actividades I cuatrimestre	5
5.2	Herramientas utilizadas	5
6.	CONCLUSIONES	5

## 1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información es un instrumento fundamental para proteger los activos de información y recursos tecnológicos de la Entidad frente a amenazas que puedan comprometer su confidencialidad, integridad, disponibilidad y privacidad. Este plan se fundamenta en el resultado del análisis de riesgos realizado, el cual permite identificar las vulnerabilidades y amenazas que podrían afectar la información de los procesos del IDARTES.

A través de este plan, se establecen medidas y controles específicos orientados a mitigar los riesgos detectados, garantizando así la continuidad de los servicios, el cumplimiento de los objetivos institucionales y el fortalecimiento de la confianza en el manejo de la información. Su implementación se basa en las mejores prácticas y lineamientos en materia de seguridad de la información.

## 2. OBJETIVO

Presentar los resultados del seguimiento y monitoreo realizados durante el primer cuatrimestre del año en curso sobre la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el fin de evidenciar el avance en la implementación de los controles para mitigar los riesgos identificados, fortalecer la protección de los activos de información de la Entidad y garantizar la continuidad y seguridad de la operación y servicios.

## 3. ALCANCE

Este informe presenta los resultados de las actividades ejecutadas durante el primer cuatrimestre del año, en el marco del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto, incluye el seguimiento y monitoreo del cumplimiento de las metas y productos programados en dicho plan.

## 4. RESPONSABLES

A continuación, se presentan los roles y responsabilidades claves que participan en la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, alineado con las buenas prácticas y las normativas vigentes en la materia:

ROL	RESPONSABILIDAD
Comité Institucional de Gestión y Desempeño	Aprobar el plan, asignar recursos y hacer seguimiento a los resultados.
Oficina Asesora de Planeación y Tecnologías de la Información – OAPTI.	Implementar la política institucional de gestión de riesgos y seguridad digital.
Referente de Seguridad de la Información.	Coordinar la implementación del plan, realizar análisis de riesgos y proponer verificar la aplicación de controles.
Responsables de los activos de información	Aplicar las medidas de seguridad de los activos de información bajo su responsabilidad y custodia.
Oficina de Control Interno	Realizar auditorías y seguimiento al cumplimiento del MSPI y el monitoreo de los riesgos de seguridad de la información.

ROL	RESPONSABILIDAD
Usuarios Institucionales	Cumplir las políticas, reportar los incidentes o eventos de seguridad de la información, aplicar los procedimientos y participar en las diferentes capacitaciones de seguridad de la información establecidos.

Tabla 1. Roles y responsabilidades Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

## 5. RESULTADOS DEL MONITOREO I CUATRIMESTRE

En el marco del seguimiento y monitoreo de las actividades programadas para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, a través del Plan de Acción Integral, correspondiente al primer cuatrimestre del presente año, se reporta un avance del 25% en la ejecución, frente a una meta establecida del 33% conforme a la programación cuatrimestral. No obstante, se identificó que una de las cuatro actividades no presentó avances en su ejecución durante el primer cuatrimestre. Esta situación obedece a que la formulación de la gestión de la demanda requiere ser articulada con la capacidad actual de la infraestructura tecnológica, proceso que está previsto para su desarrollo a partir del segundo semestre del año.

Se continuará realizando el seguimiento y monitoreo periódico para asegurar que esta actividad pendiente, sea iniciada acorde a la planeación realizada, garantizando así el cumplimiento de los objetivos establecidos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

ACTIVIDAD	PRODUCTO	% AVANCE I CUATRIMESTRE	PLAZO DE CUMPLIMIENTO
1. Revisar y actualizar el mapa de riesgos de seguridad de la información de acuerdo con la planeación de la OAPTI.	1 Mapa de riesgos de seguridad de la información.	33%	31/12/25
2. Ejecutar análisis periódicos de vulnerabilidades en los sistemas de información y/o recursos tecnológicos de la Entidad para identificar, evaluar y mitigar posibles debilidades de seguridad que puedan ser explotadas por amenazas internas o externas.	3 informes de vulnerabilidades realizados por	33%	31/12/25
3. Revisar y monitorear la infraestructura tecnológica utilizando la herramienta de monitoreo de eventos designada para este propósito.	3 Informes de monitoreo de eventos de la infraestructura tecnológica.	33%	31/12/25
4. Documentar la gestión de la demanda de capacidad de Infraestructura de TI.	1 Documento de la gestión de la demanda de capacidad.	0%	31/12/25

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

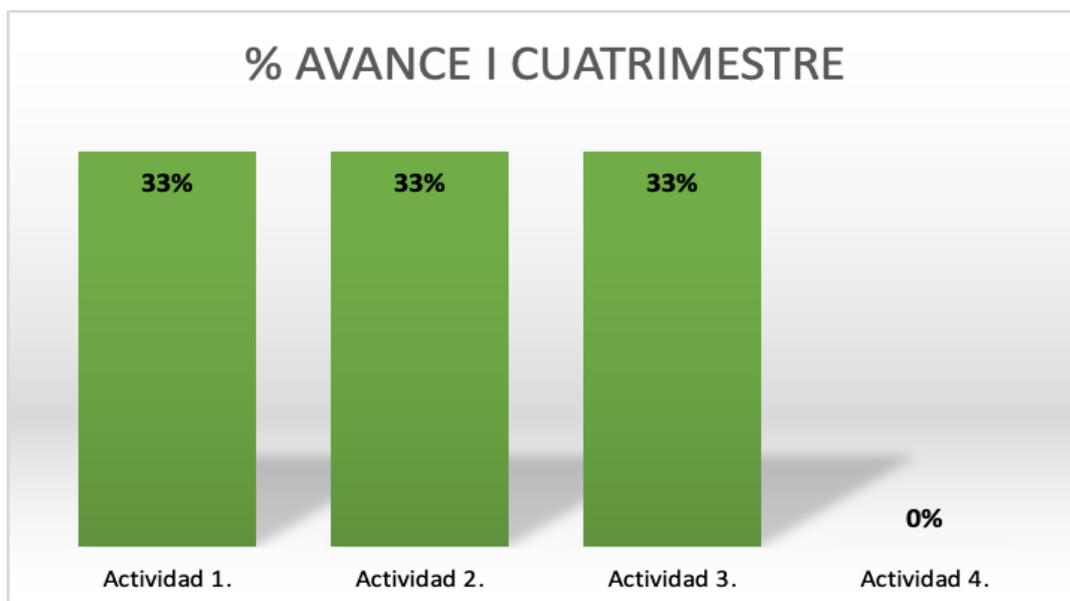


Ilustración 1. Avance Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

### 5.1 Implementación actividades I cuatrimestre

- Se realizó la actualización y el monitoreo del mapa de riesgos de seguridad de la información para el año 2025, asegurando su alineación con los activos de información y los recursos tecnológicos del IDARTES. Este proceso permite identificar oportunamente nuevas amenazas, evaluar la efectividad de los controles existentes y fortalecer las acciones de mitigación, garantizando la protección y continuidad de la operación y servicios institucionales.
- Se realizó el escaneo de vulnerabilidades a los siguientes activos de información: Sistema SIF, Orfeo, Pandora y la página web Comunicarte, la remediación de las vulnerabilidades detectadas se encuentra actualmente en proceso de gestión por parte de los responsables de cada uno de los sistemas.
- Se llevó a cabo el monitoreo continuo de la infraestructura tecnológica utilizando la herramienta especializada de gestión y monitoreo de eventos designada para este propósito.
- Se implementaron medidas preventivas mediante el bloqueo, a través del firewall perimetral, de direcciones IP identificadas como sospechosas o con actividad maliciosa hacia la entidad. Esta acción contribuye a mitigar riesgos de accesos no autorizados, intentos de intrusión y otros tipos de amenazas, fortaleciendo así la protección de los activos de información y la infraestructura tecnológica del IDARTES.

### 5.2 Herramientas utilizadas

Para realizar el seguimiento del avance correspondiente al primer cuatrimestre, en relación con los productos definidos en las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se utiliza un instrumento en Excel que fortalece el autocontrol, el seguimiento y la mejora continua de las acciones planificadas en dicho plan.

Adicionalmente, se lleva a cabo un seguimiento permanente del mapa de riesgos de seguridad de la información, lo que permite evaluar la efectividad de los controles implementados y de las acciones definidas para el tratamiento de riesgos.

## 6. CONCLUSIONES

- Fortalecimiento de la gestión de los riesgos de seguridad de la información, la implementación del plan permite a la entidad gestionar de manera metódica y eficiente los riesgos que amenazan la confidencialidad, integridad y disponibilidad de sus activos de información, garantizando así un entorno más seguro y controlado.
- A través del seguimiento y monitoreo de las acciones planificadas, se logra avanzar en la implementación de los controles ISO y adoptar mejores prácticas alineadas con estándares internacionales, como la norma ISO27001, contribuyendo a una mayor madurez en la gestión de la seguridad y privacidad de la información.

Elaboro: Maryury Forero Bohórquez – Contratista OAPTI  
Reviso: Jonathan González – Profesional Universitario OAPTI



Radicado: **20254300324273**

Fecha 29-05-2025 14:50

**Documento 20254300324273 firmado electrónicamente por:**

**JONATHAN GONZÁLEZ BOLAÑOS**, Profesional Universitario Código: 219 Grado: 01, Área de Tecnología, Fecha de Firma: 29-05-2025 15:26:31

**DANIEL SÁNCHEZ ROJAS**, Jefe Oficina Asesora De Planeación Y Tecnologías De La Información, Oficina Asesora de Planeación, Fecha de Firma: 29-05-2025 15:30:50

Proyectó: SANDRA PATRICIA MORENO BOHORQUEZ - TECNICO ADMINISTRATIVO - Área de Tecnología



7494a1329fcb05646d19a3ab20ba2e46f83fd3a9179950790360ee11b155253a

